REPORT OF EXAMINATION | 2020M-6

Brunswick Central School District

Online Banking

MAY 2020

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Brunswick Central School District

Audit Objective

Determine whether the Board and District officials ensured online banking transactions were appropriate and secure.

Key Findings

- The Board did not adopt an online banking policy.
- Employees accessed nonbusiness websites although it is prohibited by District policy.
- District officials did not provide IT security awareness training to IT 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.

District officials generally agreed with our recommendations and have initiated or indicated they planned to initiate corrective action.

Background

The Brunswick Central School District (District) serves the Towns of Brunswick, Pittstown, Grafton, Poestenkill and Schaghticoke in Rennselaer County.

The District is governed by a nine-member Board of Education (Board). The School Superintendent (Superintendent) is the District's chief executive officer. She is responsible, along with other administrative staff, for the District's day-to-day management.

The District's Assistant Superintendent of Business, Treasurer and Deputy Treasurer were responsible for overseeing and performing online banking activity.

Quick Facts	
Online Banking Computers	3
Online Banking Transactions During our Audit Period	307
Bank Account Balance with Online Access, as of September 30, 2019	$4,430,554

Audit Period

July 1, 2017 – September 30, 2019

Online Banking

How Should District Officials Safeguard Online Banking Transactions?

Online banking provides a way to directly access funds held in the District's bank accounts. Users can review current account balances and account information, including recent transactions, and transfer money between accounts or to external accounts. New York State General Municipal Law (GML)[1] allows school districts to disburse or transfer funds by electronic funds transfers (EFTs), provided that the governing board enters into a written agreement with the district's 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.

The District 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.

District Officials Did Not Adequately Safeguard Online Banking Transactions

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 told us they were unaware that GML required the District to have an online banking agreement with its bank. Without an adequate online banking agreement, officials cannot ensure that authorized employees will understand their roles when performing online bank transactions.

While officials properly segregated duties for processing online banking transactions by requiring the Treasurer to obtain secondary approval of all

1 General Municipal Law, Article 2, Section 5-A

EFTs from the Deputy Treasurer or Assistant Superintendent of Business, District officials did not ensure that a dedicated computer was used for these transactions. Instead, the three online banking users conducted online banking on the District computers assigned to them, which they used for all other work-related activities, including connecting to the Internet.

However, during our fieldwork, District officials set up a new computer to be used specifically for online banking. 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 Acceptable Use Policy Secure and Protect the District's IT Systems?

A school district should have an acceptable computer use policy (AUP) that defines the procedures for computer, Internet and email use. The policy also 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 malware that may compromise data confidentiality, integrity or availability. District officials can reduce the risks to personal, private and sensitive information (PPSI)[2] 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 the acceptable use policy. 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.

In addition, officials should require employees to sign acknowledgement forms to indicate they read the District's AUP and were aware of what was expected of them and to acknowledge they would be held accountable to the policies and procedures outlined in the AUP. The District's AUP requires IT users to sign an acknowledgment form indicating that they are aware of and will comply with the District's AUP.

2 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.

Officials Did Not Monitor For AUP Compliance

District officials did not monitor employee Internet use or implement procedures to monitor for compliance with the District's AUP. We reviewed the web browsing histories on the three computers used for online banking and found that the users assigned to these computers accessed websites for nonbusiness purposes that were prohibited by the District's AUP.

Specifically, employees accessed websites for personal commercial purposes, such as shopping, banking and bill payment websites, and non-District related activities, such as watching videos or browsing entertainment news and blogs. Also, officials did not implement any controls to prevent users from accessing non-District related websites, such as installing web filtering software to prevent access to these websites.

In addition, officials could not provide us with evidence that all network users had read, were aware of and acknowledged they would be held accountable to the AUP. The Assistant Superintendent of Business and Treasurer both signed an AUP acknowledgment form and, as a result, they should have been aware they were in violation of the District's policy. However, the Deputy Treasurer did not have a signed AUP acknowledgment 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 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, such as phishing,[3] and computer viruses and other types of malicious software that could compromise online bank 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.

3 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. Phishing attacks could use fake email messages pretending to represent a bank that request information such as name, password and account number and provide links to a fake website.

The training should also 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 Board and officials should establish a policy and written procedures that require employees to be trained in IT security awareness issues and in proper usage of the IT infrastructure, software and data. While IT policies will not guarantee the safety of the 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. The District's AUP requires the Superintendent, or his or her designee, to provide staff with training in the proper and effective use of the District's computer resources.

Officials Did Not Provide IT Security Awareness Training

District officials did not provide users of online banking services with IT security awareness training to help ensure they understand IT security measures designed to safeguard the District's financial assets from potential abuse or loss and understand their role in protecting District assets. While the District's Network Administrator periodically sent emails to IT users informing them about reported or known cybersecurity threats, officials did not provide any formal training.

In March 2018, the District administered a fake phishing email test[4] to all District network users, which included users of the online banking services. Thirty-three individuals interacted with the phishing email, including the Assistant Superintendent of Business and Treasurer. The Assistant Superintendent told us she was aware of the test and wanted to click the link to see what it looked like. However, the Treasurer entered information as requested by the phishing email.

There was no follow-up training provided to any of the individuals who interacted with the phishing email because the Network Administrator did not think it was necessary. But given the potential risks involved with District employees interacting with phishing emails and the high number of employees who responded to the fake phishing email, we feel training was warranted to help minimize the risks to the District's computer system and online bank accounts.

Because District officials did not provide IT security awareness training or restrict personal use of District computers used for online banking, District funds were vulnerable to online theft through unauthorized access. We reviewed all 307

4 The test was administered to all District network users. It sent a fake email message impersonating a District employee who asked users to enter their emergency contact information into a Google sheets document and required users to input their email account's login credentials into a phishing link.

EFTs totaling $51.9 million generated during our audit period and found they were for appropriate District purposes. However, if the District's bank accounts were attacked and funds were misappropriated, the District could have lost up to $3.4 million[5] as of September 2019.

The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. District officials cannot protect the confidentiality, integrity and availability of data and computer systems without ensuring that users, or those who manage IT, understand the IT security policies and procedures and their roles and responsibilities related to IT and data security.

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, data, PPSI, IT assets and District financial assets could be at greater risk for unauthorized access, misuse or loss.

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 This amount would include losses incurred after funds transfer fraud insurance deductions.

Appendix A: Response From District Officials

BRUNSWICK CENTRAL SCHOOL DISTRICT
OFFICE OF THE SUPERINTENDENT
Dr. Angelina Maloney

April 7, 2020

Mr. Gary Gifford
Chief Examiner
NYS Office of the State Comptroller
Division of Local Government and School Accountability
One Broad Street Plaza
Glens Falls, NY 12801

Re: Brunswick Central School District
Online Banking 2020M-6

Dear Mr. Gifford

This is a response to the audit conducted by the Office of the State Comptroller for the Brunswick Central School District. This will also serve as the District's Corrective Action Plan.

The District is in general agreement with the findings from the audit.

The District has already addressed several of the key findings in the report.

Online Banking Policy

Audit Recommendation: The Board should adopt a comprehensive online banking policy.

The district agrees that an online banking policy should be adopted. The district has already brought an online banking policy to the policy committee for discussion. An online banking policy will be adopted in the near future.

IT Security Awareness Training

Audit Recommendation: The Superintendent should ensure that all IT users, especially those involved with district online banking, are provided with formal IT security awareness training.

The district agrees that further IT security awareness training could benefit the employees of the district. While the district did conduct an IT fake phishing email test a few years ago, the District will look to conduct a more thorough and comprehensive training on a yearly basis with all of our employees.

District Acceptable Use Policy

Audit Recommendation: District Officials should monitor computer use to ensure compliance with the AUP and regulations.

The district agrees. The district has already adjusted our web filtering to comply with the district's AUP.

Audit Recommendation: District Officials should ensure all IT users sign an acknowledgement form indicating that they are aware of and will comply with the District's AUP.

The district agrees. The district has already ensured that the acceptable use policy and an acknowledgement form is placed in the new hire paperwork for all new employees.

The District would like to thank the Office of the State Comptroller for their recommendations to improve our District operations.

Please feel free to reach out to me with any questions or concerns.

Sincerely,

Angelina Maloney

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 gain an understanding of online banking practices and to obtain any related policies and procedures.
- We reviewed District policies relating to acceptable Internet use.
- We reviewed AUP acknowledgement forms for employee signatures.
- We observed all online banking users' access from logon to logoff.
- We used specialized audit software to examine the three computers used for online banking purposes.
- We reviewed written agreements with the bank and online banking and EFT procedures.
- We reviewed all online banking transactions generated during our audit period to determine whether they were for appropriate District purposes.

Our audit also examined the adequacy of certain IT 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 must 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/index.htm

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

GLENS REGIONAL OFFICE – Gary G. 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

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller