REPORT OF EXAMINATION | 2022M-102

Bradford Central School District

Online Banking

DECEMBER 2022

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

Contents

Report Highlights

Bradford Central School District

Audit Objective

Determine whether the Bradford Central School District (District) officials ensured online banking transactions were appropriate and secure.

Key Findings

While we found online banking transactions were appropriate, District officials did not secure access to online banking. In addition to sensitive information technology (IT) control weaknesses that we confidentially communicated to District officials, officials did not:

- Ensure that authorized access to online bank accounts was limited.
- Have an adequate online banking policy and procedures.
- Monitor computer use with the acceptable use policy.

Key Recommendations

- Limit online banking access to only those individuals authorized by the Board.
- Update the electronic banking policy and disseminate it to all authorized online banking users.
- Designate a computer for online banking transactions.
- Periodically monitor computer use to ensure compliance with the acceptable use policy.

District officials agreed with our recommendations and indicated they will take corrective action.

Background

The District serves the Towns of Bath, Bradford, Urbana and Wayne in Steuben County and the Towns of Orange and Tyrone in Schuyler County.

The District is governed by an elected five-member Board of Education (Board) responsible for managing and controlling the District's financial and educational affairs.

The District's Business Administrator is contracted through the Greater Southern Tier Board of Cooperative Educational Services (BOCES). The Board-appointed Treasurer and Deputy Treasurer are employees of the BOCES central business office (CBO).

The Treasurer initiates bank and wire transfers using online banking. The District's purchasing clerk uses online banking to make remote check deposits. District and CBO employees use both District and BOCES network resources to perform online banking transactions.

Quick Facts	
Bank balances as of February 28, 2022	$5.4 million
Online bank transfers completed and reviewed	$16 million
Wire transfers and Automated Clearing House payments reviewed	$5.4 million
Online banking users	7

Audit Period

July 1, 2020 – June 10, 2022

Online Banking

New York State General Municipal Law (GML) Section 5-a allows school districts to disburse or electronically transfer funds, provided that the governing board has entered into a written agreement with the bank. This agreement must:

- Prescribe the manner in which electronic or wire transfers of funds will be accomplished,
- Identify the names and numbers of the bank accounts from which such transfers may be made,
- Identify the individuals authorized to request the transfer of funds, and
- Implement a security procedure that includes verifying that a payment order is the initiating entity's and detecting errors in transmission or content of the payment order.

Online banking also provides a means of monitoring and accessing funds held in school district bank accounts. Users can transfer money between bank accounts and to external accounts and review account balances and account information.

How Can Officials Secure and Reduce the Risk of Inappropriate Online Banking Transactions?

School districts should establish online banking controls that help prevent unauthorized transfers and inappropriate transactions from occurring. It is essential that school district officials authorize transfers before they are initiated and establish procedures to ensure that staff are securely accessing banking websites.

To safeguard cash assets, a board should adopt comprehensive written online banking policies and procedures to monitor and control online banking transactions. A comprehensive written online banking policy should:

- Clearly describe the online activities school district officials may perform,
- Specify which employees are authorized to process transactions,
- Establish a detailed approval process to verify the legitimacy and accuracy of transfer requests, and
- Require the review and reconciliation of transactions.

School district officials should segregate the duties of employees granted access to online banking applications to ensure that employees are unable to perform all phases of a financial transaction on their own. Someone independent of the online banking transactions must frequently monitor the activity to identify unauthorized or suspicious activity.

Good management practices should limit the number of users authorized to execute online banking activities and the number of computers used.

Authorized online banking users should only access bank accounts from one computer (if possible) dedicated for online banking transactions. This helps minimize potential exposure to malicious software and other unauthorized access because a dedicated computer could have an isolated Internet connection, be locked up after each use and be connected to the Internet with a physical cable rather than wirelessly. With the increased security protections afforded by a dedicated computer, online banking transactions executed from this computer could be less at risk.

Officials should monitor and enforce their acceptable use policy (AUP). The District's AUP states that activities of a curricular and professional nature have priority over those oriented toward personal growth and self-discovery. It further states that technology resources should be used in compliance with the educational goals set by the Board and details specific activities and practices that are not allowed. The BOCES AUP also restricts personal use of BOCES IT assets.

Employees and officials with online banking access should also receive Internet security awareness training to educate them on safe computing practices, such as avoiding untrusted websites.

District Officials Did Not Secure Online Banking Transactions

District officials did not ensure that authorized access to the District's online bank accounts was limited to those individuals authorized by the Board's electronic banking policy. The Board-adopted electronic banking policy authorized the Treasurer and, in their absence, the Deputy Treasurer, to transmit wire or electronic fund transfers. The electronic banking policy also states that the Administrator or Treasurer shall approve and release electronic banking requests, such as payroll deposits, debt payments and purchase order payments. However, we found that the Business Administrator was not provided online banking access as required, and five unauthorized individuals were provided online banking access to the District's two bank accounts (Figure 1).

Figure 1: Users With Online Banking Access

Title	Bank 1	Bank 2
Treasurer	X	X
Deputy Treasurer	X	X
CBO Employee	X	
CBO Accountant	X	X
Purchasing Clerk	**X**	
District Clerk	X	
Extra-Classroom Treasurer	X	

The Treasurer stated that she was not provided the electronic banking policy and added or removed online banking users as needed. For example, the purchasing clerk and District Clerk were added to make remote deposits at Bank 1. However, the Treasurer was not authorized to add or remove users at will.

Although three of the additional five individuals have not accessed the District's online banking websites in the last three years, stale online banking user accounts are a significant security issue, as external attackers could use those user accounts to make fraudulent online banking transactions.

- The extra-classroom treasurer did not have their online banking access removed from Bank 1 when the extra-classroom funds were transferred to Bank 2. The extra-classroom treasurer was not given online banking access to Bank 2.
- The CBO employee previously used his online banking access to perform bank reconciliations for the District.
- The District Clerk serves as the purchasing clerk's backup for performing remote check deposits. However, the electronic banking policy does not address the remote deposit of checks at Bank 1 or the individuals authorized to perform the procedure. We note that Bank 2 is not set up for remote deposit.

All seven individuals generally used their District or BOCES assigned computer to perform their regular day-to-day job duties and accessed the online banking websites instead of a designated computer. However, the scanning machine for remote deposits is only attached to the purchasing clerk's computer, so the District Clerk would need to use it to perform the remote deposits in the purchasing clerk's absence.

The District's electronic banking policy did not indicate who is responsible for reviewing and reconciling online banking transactions or how often this should be done. Additionally, it does not provide procedures for responding to potentially fraudulent activities. However, we note that the CBO employee completed monthly bank reconciliations, and the Deputy Treasurer or CBO Accountant reviewed and approved wire transfers from Bank 1.

District officials, including the Business Administrator, did not review the wire transfer confirmations that Bank 2 mailed to the District for appropriateness and accuracy. Instead, the purchasing clerk sent them to the Treasurer at the CBO who compared the amount listed on the wire transfer confirmations to her records before throwing them away.

We reviewed all online bank transfers between July 1, 2020 and February 28, 2022 totaling approximately $16 million, and wire transfers and Automated Clearing House (ACH) payments for the months of June and December 2021

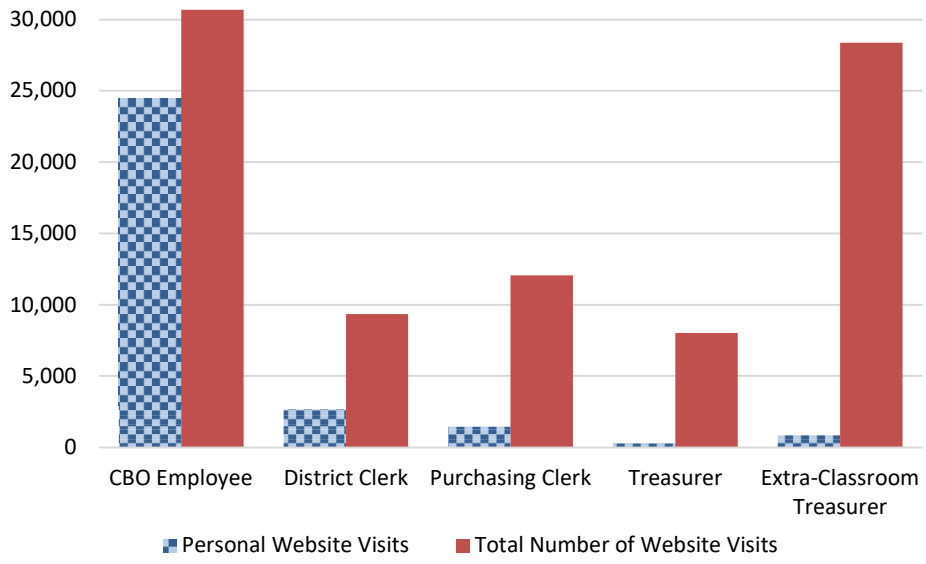
totaling about $5.4 million. We found that the online bank transfers, wire transfers and ACH payments were for appropriate purposes.

Because we identified certain sensitive IT security weaknesses related to District officials' online banking practices and the users with online banking access could not recall that they were provided cybersecurity training, we also reviewed the web browsing history on the seven computers assigned to the users with online banking access.

The Deputy Treasurer and CBO Accountant had minimal web browsing activity, while the other five online banking users generally had three months of web browsing activity stored. We found excessive personal Internet use by the CBO employee, District Clerk and purchasing clerk, and incidental personal Internet use by the Treasurer and extra-classroom treasurer (Figure 2). All personal web browsing activities were prohibited by the District's and BOCES' acceptable use policies.

FIGURE 2

Personal Website Use



These individuals accessed websites for personal Internet use, including websites for:

- Shopping,
- News,
- Sports and entertainment,
- Streaming music,
- Personal banking,
- Email and bill payments,
- Hobbies, and
- Outside bookkeeping services.

Because acceptable use was not monitored by District officials, individuals used their assigned computers for personal purposes, which increases the risk of malicious software and attacks on the computer systems and decreases employee productivity.

We recognize that District officials took measures to limit potential financial loss by purchasing computer fraud and funds transfer insurance coverage. Although this may not prevent the District's initial financial loss in the event of online banking fraud, it may provide some financial reimbursement from actual losses in accordance with the insurance policy. However, dedicating a computer for online banking and providing continued Internet security training for those involved in online banking transactions can help reduce the District's risk of funds being misappropriated due to a malicious software infection or unauthorized access.

What Do We Recommend?

The Board should:

1. Update the electronic banking policy to include procedures for the remote deposit of checks if this practice is acceptable, and who is responsible for reviewing and reconciling online banking transactions and how often this should be done and responding to potentially fraudulent activities.

District officials should:

2. Disseminate the updated electronic banking policy to all authorized online banking users so that those who perform online banking transactions are familiar with its content.

3. Limit online banking access to only those individuals authorized by the Board.
4. Consider designating one computer to be used for all online banking transactions.
5. Ensure bank wire confirmations are reviewed by the Business Administrator.
6. Periodically monitor computer use to ensure compliance with the acceptable use policy.
7. Continue to periodically provide Internet security training.

Appendix A: Response From District Officials

BRADFORD
CENTRAL SCHOOL DISTRICT
Enter to learn, leave to succeed!

November 3, 2022

Mr. Edward V. Grant
Chief Examiner
16 West Main Street Suite 522
Rochester, NY 12236

Dear Mr. Grant,

The purpose of this correspondence is to acknowledge that the Bradford Central School District has received a draft copy of the audit conducted by the New York State Comptroller's Office regarding online banking. We agree with our findings and plan to implement procedural safeguards based upon the recommendations provided.

RECOMMENDATION IMPLEMENTATION PLAN

OSC Online Banking, Report of Examination - Bradford Central School District

July 1, 2020 – June 10, 2022

Recommendation

The Board should:

1. Update the electronic banking policy to include procedures for the remote deposit of checks if this practice is acceptable, and who is responsible for reviewing and reconciling online banking transactions and how often this should be done and responding to potentially fraudulent activities.

Implementation Action(s)

The Board of Education is in the process of updating the entire Policy Manual and will have updated all policies by the end of the 2022-23 year. The electronic banking policy will be updated to include remote deposit procedures, identify those responsible for reviewing and reconciling online banking transactions, the frequency of this review, and response to potentially fraudulent activities.

Implementation Date: by June 30, 2023

2820 State Route 226, Bradford, NY 14815 • Phone: 607-583-4616 • Fax: 607-583-4013
www.bradfordcsd.org

Person(s) Responsible for Implementation: Board of Education, Superintendent John Marshall, and School Business Administrator Lisa Kuhnel

Recommendation

District officials should:

2. Disseminate the updated electronic banking policy to all authorized online banking users so that those who perform online banking transactions are familiar with its content.

Implementation Action(s)

Once the electronic banking policy has been updated and approved by the Board of Education, it will be distributed to all authorized online banking users.

Implementation Date: by June 30, 2023

Person(s) Responsible for Implementation: School Business Administrator Lisa Kuhnel

Recommendation

District officials should:

3. Limit online banking access to only those individuals authorized by the Board.

Implementation Action(s)

Access to online banking has already been removed for two unauthorized users. It is necessary for other current users to maintain access to complete District business. These users will be authorized in the updated Board policy.

Implementation Date: by June 30, 2023

Person(s) Responsible for Implementation: Board of Education, Superintendent John Marshall, and School Business Administrator Lisa Kuhnel

Recommendation

District officials should:

4. Consider designating one computer to be used for all online banking transactions.

Implementation Action(s)

BRADFORD
CENTRAL SCHOOL DISTRICT
Enter to learn, leave to succeed!

The District will install a hardwired computer to be used solely for the purpose of online banking transactions. This device will be set up with a unique login with no ties to any other staff accounts.

Implementation Date: by June 30, 2023

Person(s) Responsible for Implementation: Technology Director Dylan Blencowe

Recommendation

District officials should:

5. Ensure bank wire confirmations are reviewed by the Business Administrator.

Implementation Action(s)

The Business Administrator will review bank wires on a monthly basis.

Implementation Date: immediately

Person(s) Responsible for Implementation: School Business Administrator

Recommendation

District officials should:

6. Periodically monitor computer use to ensure compliance with the acceptable use policy.

Implementation Action(s)

The District will monitor computer use semi-annually to ensure compliance with the acceptable use policy. A semi-annual report from the Technology Department will be issued to the Superintendent to report compliance issues.

Implementation Date: by June 30, 2023

Person(s) Responsible for Implementation: Technology Director Dylan Blencowe

Recommendation

District officials should:

7. Continue to periodically provide Internet security training

2820 State Route 226, Bradford, NY 14815 • Phone: 607-583-4616 • Fax: 607-583-4013
www.bradfordcsd.org

BRADFORD
CENTRAL SCHOOL DISTRICT
Enter to learn, leave to succeed!

Implementation Action(s)

The District will continue to use email communication that reviews internet security protocols and refreshes the annual training staff receive at the start of each year.

Implementation Date: ongoing

Person(s) Responsible for Implementation: Technology Director Dylan Blencowe

The Bradford Central School District would like to thank the New York State Comptroller's Office for their high level of professionalism and the thorough work done while auditing our district.

Sincerely,

[redacted]

John R. Marshall
Superintendent

2820 State Route 226, Bradford, NY 14815 • Phone: 607-583-4616 • Fax: 607-583-4013
www.bradfordcsd.org

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 and CBO staff to obtain an understanding of online banking practices and to obtain any related policies and procedures.
- We reviewed policies and procedures for acceptable use of information technology and online banking.
- We observed online banking users' access from logon to logoff for the seven users with online banking access.
- On March 9, 2022, March 15, 2022 and March 16, 2022, we ran a computerized audit script to export the web history files from the seven computers assigned to the seven users that had online banking access. We then examined the exported web history data for indications of personal Internet use.
- We inquired with District officials about a written agreement with the bank and reviewed the documentation they provided us regarding capabilities for electronic transfers.
- We reviewed all wire transfers and ACH debits for the judgmentally selected months of June 2021 and December 2021 because bond payments were made in those months.
- We reviewed all online transfers during the period of July 1, 2020 through February 28, 2022.

Our audit also examined the adequacy of certain sensitive 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/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/files/local-government/publications/pdf/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/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications

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

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/local-government

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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief of Municipal Audits

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

Serving: Cayuga, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

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