REPORT OF EXAMINATION | 2018M-79

Bath Central School District

Online Banking

JULY 2018

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

Contents

Report Highlights

Bath Central School District

Audit Objective

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

Key Findings

- Officials lacked adequate bank agreements for online banking transactions.
- The Board did not adopt an online banking policy and officials did not develop procedures to adequately segregate online banking duties.
- Officials did not ensure that authorized access to online bank accounts was limited or provide users with cyber security training.

In addition, sensitive information technology (IT) control weaknesses were communicated confidentially to District officials.

Key Recommendations

- Obtain adequate bank agreements and become familiar with them.
- Adopt online banking policies and procedures.
- Designate one computer to be used strictly for online banking transactions.
- Address the IT recommendations communicated confidentially.

Background

The Bath Central School District (District) serves the Towns of Avoca, Bath, Cameron, Thurston, Urbana and Wheeler in Steuben County.

The District is governed by a Board of Education (Board), which is composed of seven elected members.

The District Treasurer (Treasurer) processes online banking transactions and the central student activities treasurer (central treasurer) makes remote deposits for extracurricular activity funds. The District uses network resources to perform online banking transactions. The IT Director is responsible for managing the security of this network and the data it contains.

Quick Facts	
Employees	350
Enrollment	1,500
2017-18 Appropriations	$36.7 Million
Bank Balances as of February 28, 2018	$11.9 Million

Audit Period

July 1, 2016 – March 21, 2018

Online Banking

Online banking provides a means of direct access to funds held in district accounts. Users can review current account balances and account information, including recent transactions, and transfer money between bank accounts and to external accounts. Because wire transfers of funds typically involve significant amounts of money, districts must control the processing of its wire transfers to help prevent unauthorized transfers from occurring. It is essential that district officials authorize transfers before they are initiated and establish procedures to ensure that staff are securely accessing banking websites to help reduce the risk of unauthorized transfers from both internal and external sources.

How Should Officials Transfer Funds Using Online Banking?

New York State General Municipal Law (GML)[1] allows school districts to disburse or transfer funds in their custody by means of electronic or wire transfers, provided that the governing board has entered into a written agreement. GML requires that this agreement prescribe the manner in which electronic or wire fund transfers will be accomplished and identify the names and numbers of bank accounts from which such transfers may be made and the individuals authorized to request the transfers. In addition, GML requires the district to implement a security procedure that includes verifying that a payment order is for the initiating district and detecting payment order errors in transmission or content.

Officials Lacked Adequate Banking Agreements

District officials maintain accounts with four banks used for online transactions, which include electronic and external wire transfers, remote deposits and automated clearing house (ACH) payments.[2] The Treasurer did not have any banking agreements on hand for the three banks she conducted online transactions with, but obtained them from the banks upon our request. The central treasurer provided us with the agreement from the bank that she makes remote deposits with. While these agreements provided information on the capabilities for performing electronic transfers, the bank account numbers, names of authorized users, dollar limit for electronic payments or other details, which should be included in accordance with GML, were not included.

In addition, officials did not establish security controls with all the banks for online banking, such as secondary authorizations for online transfers, wire transfers and ACH debits. Although secondary authorization is required by one bank for wire transfers, the Treasurer is the initiator and a secondary authorizer. Without adequate online banking agreements, District officials cannot be assured that funds are adequately safeguarded when processing these transactions.

1 New York State General Municipal Law, Section 5-A

2 The ACH is an electronic network used to process large volumes of electronic payments between banks. District officials generally use ACH payments for payroll, reimbursements and prescriptions.

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

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 describes the online activities district officials will engage in, specifies which employees are authorized to process transactions and establishes a detailed approval process to verify the accuracy and legitimacy of transfer requests. Officials must properly segregate the duties of employees granted access to the online banking applications to ensure that employees are unable to perform financial transactions on their own.

Good management practices require limiting 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 because the other computers may not have the same security protections as a dedicated computer, and transactions executed from those computers could be more at risk.

An acceptable use policy should inform users about appropriate and safe computer use and users should receive cybersecurity awareness training to ensure they are aware of potential threats such as unknowingly downloading unwanted or malicious software or clicking on links that are part of phishing attacks,[3] which can threaten online bank accounts. When computer users visit personal or nonbusiness sites this risk is heightened.

Officials Did Not Safeguard Online Banking Transactions

The Board did not adopt an online banking policy and officials did not adequately segregate online banking duties. In addition, officials did not ensure that authorized access to online bank accounts was limited because a dedicated separate computer was not used for these transactions, personal computer use was not limited and users were not provided cybersecurity awareness training.

While both the Treasurer and Deputy Treasurer (Deputy) are authorized to make online banking transactions, the Deputy did not initiate any of these transactions during our audit period. The central treasurer is authorized to make remote online deposits using her assigned computer. Although the Treasurer is required to use a token[4] when making online transactions, which limited unauthorized access from outside sources, both these individuals performed these transactions with no oversight.

3 Phishing attacks use fake email messages pretending to represent a bank. The email requests information such as name, password and account number and provides links to a fake website.

4 Token identifications contain a number series assigned to a specific user.

The central treasurer receives the bank statements and prepares monthly bank reconciliations for all accounts from the four banks, but she does not review and verify the appropriateness of the online transfers between accounts or ACH payments made by the Treasurer. In addition, while the Business Administrator reviewed the bank statements and reconciliations for the online accounts used by the Treasurer, the review did not include verifying the appropriateness of online transfers. Further, no one performed an independent review of the central treasurer's extracurricular bank statements and reconciliations. As a result, District officials do not have an independent review designed to detect inappropriate online activity and such transactions could go undetected and remain uncorrected.

We reviewed two months of online banking, wire transfer and ACH transactions and found that the 76 transactions totaling $15.8 million made during this time were for appropriate purposes. However, because District officials did not provide cybersecurity training or limit personal use of District computers, we reviewed the website browsing histories on the Treasurer's, Deputy's and central treasurer's computers.

We identified questionable personal use on all these computers. Users accessed websites for online gaming, shopping, social media, travel, news and entertainment, job searches, radio streaming, personal bill paying and unauthorized education courses. Allowing personal use of computers increases the risk of malicious software and attacks on the computer system and can decrease employee productivity.

Without a formal policy that explicitly conveys practices to safeguard District assets during online banking transactions and the appropriate use of IT equipment, District officials cannot ensure that employees are aware of their responsibilities. Further, the lack of cybersecurity awareness training and a dedicated online banking computer could result in users unintentionally exposing the online bank accounts to threats from malicious software, which could subject cash assets to misappropriation.

What Do We Recommend?

The Board should:

1. Adopt a comprehensive online banking policy.
2. Consider amending the acceptable use policy to define appropriate personal computer use and inform users about safe computer use.

District officials should:

3. Ensure that the written agreement with each bank is sufficient and that those who perform online banking transactions are familiar with its content.
4. Enable notifications and other security measures available from the banks, including secondary approvals and email notifications every time an online transaction occurs.
5. Adequately segregate online banking duties.
6. Designate a computer to be used for online banking transactions.
7. Ensure that officials and employees receive adequate cybersecurity awareness training and training on online banking and IT policies.
8. Monitor computer use to ensure compliance with the acceptable use policy and regulations.

Appendix A: Response From District Officials

BATH CENTRAL SCHOOL DISTRICT
Home of the Haverling Rams

25 Ellas Avenue ▪ Bath, New York 14810
www.bathcsd.org

Joseph L. Rumsey
Superintendent of

July 2, 2018

Mr. Edward V. Grant Jr.
Chief Examiner of Local Government and School Accountability
Office of the New York State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, NY 14614-1608

RE: Bath CSD Response to Comptroller's Report

Dear Mr. Grant,

The Bath Central School District is in receipt of the June 2018 Report of Examination from your office. We would like to thank the field team from your office for their professionalism while conducting their duties during this audit. Please accept this letter as the District's official response AND corrective action plan.

Once the District learned the specifics of this report during the audit process, the District started phase two of its program by improving its procedures going forward and to remedy the problems the initial phase had revealed. In response to your recommendations, the following steps have already been completed and/or are in process and will be completed in the near future:

Policy--The Board of Education has begun the process of creating a *Comprehensive Online Banking Policy*. Under the advice and recommendations of our school attorney, this policy will receive final review and formal adoption at the August 2018 Board meeting. Additionally, the Board will be amending the District's *Acceptable Use Policy* to better define appropriate personal computer use and to better inform users about safe computer use. Although not a recommendation from the audit team, the Board of Education has also begun reviewing and amending cybersecurity and other pertinent IT policies.

Agreements and Procedures—District Officials have already completed written agreements with each bank and have revised procedures with those who perform online banking transactions. These procedural changes have increased security measures and notifications, segregated online banking duties, and is inclusive of secondary approvals/written email notifications every time an online transaction occurs. The District has provided an isolated computer used exclusively for online banking duties. The District has also planned additional cybersecurity awareness trainings for all employees to be completed on Superintendent's Conference Days in the upcoming school year. The employees will receive a digital sign-on message summarizing the acceptable use policy with notifications that all computer use is monitored regularly. The employee will not be able to sign on to his/her computer without agreeing to this notification.

Finally, as an additional step of transparency and security practice, the Board will focus the 2018-19 Internal Audit on ensuring that the District has tightened up cybersecurity measures. This will include limiting network permissions, removing and/or disabling unnecessary network accounts, enforcing stronger computer network password and lockout procedures, revising computer settings to automatically delete temporary Internet files, and to disable all services that are unnecessary for District operations.

Once again, we thank you for your professional work with our office. We look forward to answering any questions and/or providing any further documentation of our efforts in the future.

Respectfully,

Joseph Rumsey
Superintendent of Schools

Michael Mishook
President-Bath CSD Board of Education

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 and to obtain any related policies and procedures.
- We reviewed policies and procedures for acceptable use.
- We observed online banking users access from logon to logoff for both the Treasurer and the central treasurer.
- We inquired about written agreements with banks and reviewed the documentation regarding capabilities for electronic transfers.
- We examined the three computers for users that had access to online banking.
- We reviewed all online banking transactions for two months to determine whether they were appropriate District expenditures. We selected the two most recently completed months, which were January and February 2018.

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 GAGAS (generally accepted government auditing standards). 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 relevant population size and the sample selected for examination.

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 2116-1(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 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. We encourage the Board to make the CAP available for public review in the Clerk's office.

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/lgli/pdf/cybersecurityguide.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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner

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, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

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