Office of the New York State Comptroller

Division of Local Government
& School Accountability

East Bloomfield Central School District

Online Banking

Report of Examination

Period Covered:

July 1, 2014 – December 9, 2015

2016M-14

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

May 2016

Dear School District Officials:

A top priority of the Office of the State Comptroller is to help school district officials manage their districts efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support district operations. The Comptroller oversees the fiscal affairs of districts statewide, as well as districts' compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving district operations and Board of Education governance. Audits also can identify strategies to reduce district costs and to strengthen controls intended to safeguard district assets.

Following is a report of our audit of the East Bloomfield Central School District, entitled Online Banking. This audit was conducted 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.

This audit's results and recommendations are resources for district officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

Office of the State Comptroller
Division of Local Government
and School Accountability

Introduction

Background

The East Bloomfield Central School District (District) is located in the Towns of Bristol, Canandaigua, East Bloomfield, Richmond, Victor and West Bloomfield in Ontario County. The District is governed by the Board of Education (Board), which is composed of seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools is the District's chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction. The District's Treasurer is responsible for completing the banking transactions. The Business Office Clerk is responsible for payroll transfers. The School Business Administrator is responsible for overseeing these transactions.

The District operates two schools with approximately 970 students and 200 employees. The District's budgeted appropriations for the 2015-16 fiscal year are $20.2 million, which are funded primarily with State aid, sales tax, real property taxes and grants.

The District uses network resources for performing online banking transactions. The District's Information Technology Director is responsible for managing the security of this network and the data it contains. The Board is responsible for establishing policies to help ensure that security over the network and data is maintained.

Objective

The objective of our audit was to determine if online banking transactions were safeguarded. Our audit addressed the following related question:

- Did District officials ensure online banking transactions were appropriate?

Scope and Methodology

We examined the District's online banking practices for the period July 1, 2014 through December 9, 2015. We also examined information technology (IT) controls over certain District functions. 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 our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit are included in Appendix B of this report. 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.

Comments of District Officials and Corrective Action

The results of our audit and recommendations have been discussed with District officials, and their comments, which appear in Appendix A, have been considered in preparing this report. District officials generally agreed with our recommendations and indicated they planned to take corrective action.

The Board has the responsibility to initiate corrective action. 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, 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, with a copy forwarded to 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 Board should make the CAP available for public review in the District Clerk's office.

Online Banking

Online banking provides a means of direct access to moneys held in the District's accounts. It is an immediate way to review current account balances and account information, including recent transactions, and to transfer moneys between bank accounts and to external accounts. School districts are allowed to disburse or transfer funds in their custody by means of electronic or wire transfer. Wire transfers of funds typically involve significant amounts of money. For that reason, to help prevent unauthorized transfers from occurring, it is important to control the processing of wire transfers. Establishing appropriate procedures to securely access banking websites helps to reduce the risk of unauthorized transfers from both internal and external sources.

Appropriate controls over electronic or wire transfers include secured bank account access and management authorization of transfers before the transactions are initiated. Bank account access should be limited to necessary employees and authorization for each transfer should be supported by documentation itemizing the purpose, source, destination and amount of the transfer. A good detective control would be to require banks to provide emails or texts to District officials alerting them every time an online transaction occurs. District officials could also provide for an independent review of bank reconciliations and purchase computer fraud and funds transfer insurance coverage.

Although the Board adopted an online banking policy, District officials did not develop written procedures for online banking activities. In addition, online banking duties were not properly segregated and account accessibility was not completely controlled. Furthermore, the Treasurer and Business Office Clerk did not use proper procedures when accessing online banking sessions. Finally, the Treasurer and Business Office Clerk did not receive appropriate online banking training.

Policies and Procedures

In order to effectively safeguard District cash assets, policies and procedures are necessary to properly monitor and control online banking transactions. A comprehensive online banking policy clearly describes the online banking activities the District will engage in, specifies which District employees have the authority to process transactions and establishes a detailed approval process to verify the accuracy and legitimacy of transfer requests.

The Board adopted an online banking policy that authorizes the Treasurer to perform electronic transactions. The policy also authorizes the Business Office Clerk or Deputy Treasurer, who is the Business Administrator, to perform online banking transactions in

the Treasurer's absence. However, we found that the Business Office Clerk regularly initiated online payroll transactions. In addition, the Business Administrator told us that she does not know her online banking credentials. The Board policy also requires that procedures be implemented specifying "who is authorized to initiate, approve, transmit, record, review and reconcile electronic transactions. At least two individuals will be involved in each transaction." We found that District officials have not implemented these procedures and two individuals are not involved in each transaction.

Segregation of Duties

To adequately safeguard District assets, District officials must properly segregate the duties of employees granted access to the District's online banking application. Effective policies and procedures which segregate job duties also ensure that employees are unable to perform financial transactions unilaterally.

We found that the District has not adequately segregated employee duties related to online banking transactions. Specifically, the Treasurer has full access to all of the District's online bank accounts, which enables her to initiate and authorize transfers to and from District bank accounts without the review or authorization of any other District employee or official. In addition, the Business Office Clerk has access[1] to the District's two payroll bank accounts. Although we found that the Treasurer initiates external wire transfers via a fax that is approved by the Business Administrator, a direct confirmation is not sent to both officials. Additionally, when the Business Office Clerk initiates payroll automated clearing house (ACH) transactions, the bank texts a security code to her cell phone for verification prior to authorizing the transaction. A separate notification is not sent to a second District employee or official, such as the Business Administrator. Adding a second authorization or notification provides an added level of security over online transactions.

Although the Business Administrator is not directly involved in the online banking transactions, she receives the District's bank statements directly from the bank and reviews the bank activity in the District's computerized accounting system prior to providing the statements to the Treasurer, who prepares the bank account reconciliation. Therefore, there is a control in place to identify inappropriate activity. However, inappropriate transactions could go undetected for longer than necessary because there is about a month of time between these reviews and more than a month of online banking activity to be reviewed.

[1] Per the District's bank agreement, the Business Office Clerk's access is limited to ACH transactions. She cannot initiate wire transfers or use bill pay.

Authorized Access

Good management practices would not only limit the users authorized to execute online banking activities, but also limit the computers on which the activity can take place. Authorized online banking users should only access the District's bank accounts from one District computer dedicated for online banking transactions. Other district computers may not have the same security protections as a dedicated online banking computer, and transactions executed from those computers could be more at risk. Further, computer users who are unaware of potential threats are more likely to unknowingly download unwanted or malicious software or click on links that are part of phishing attacks,[2] which can threaten online bank accounts.

Authorized users should be assigned user names, passwords, and token identifications[3] that are user-specific and maintained in a secure place. Users should type the bank's website uniform resource locator (URL) address into the Internet's address bar every time they log-on to the application. In addition, users must always ensure the website is authentic by checking the web address and general appearance of the website and ensuring the connection is secure (secure website addresses begin with https). Additional procedures should be established to ensure that that user names and passwords meet complexity requirements. Additionally, when exiting the bank's website, users should log-out of online banking sessions because simply closing the browser window could leave District accounts open to threats.

The District has not ensured that authorized access to the District's online bank accounts was limited because a separate computer has not been dedicated just for these transactions. In addition, we noted various weaknesses when the Treasurer and Business Office Clerk accessed the online banking website that could compromise the District's bank accounts, which were discussed separately. Furthermore, the bank has not provided the District with tokens[4] for added online banking log-in security. Lastly, both the Treasurer and Business Office Clerk perform online banking transactions but neither has received internet security awareness training in about four years. This lack of training could result in users unintentionally exposing the District's online bank accounts to threats from malicious software which could endanger District assets.

---

[2] 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.

[3] Token identifications contain a number series assigned to a specific user.

[4] A token is a small security hardware device with built-in authentication used to control and secure access to network services and data. With the addition of a token, the District would be using two-factor authentication, allowing for increased security by requiring two forms of user verification (password and token).

As a result of these deficiencies, we reviewed online banking and wire transfers, as well as ACH transactions, for one month and found that all 89 transactions were for appropriate District purposes.

We recognize District officials have taken an additional and proactive step to prevent loss by purchasing computer fraud and funds transfer insurance coverage. Although this may not prevent the District's initial loss, it will provide some reimbursement from actual losses in accordance with the insurance policy.

Recommendations

District officials should:

1. Establish written online banking procedures as specified in the Board policy.

2. Designate one computer to be strictly dedicated for online banking transactions.

3. Contact the bank about adding a second log-on security feature such as a token to provide an extra level of assurance through two-factor authentication.

4. Ensure that alerts and other security measures available from the District's bank are enabled, including an alert system that advises the Administrator, Treasurer and/or Business Office Clerk by email or text every time an online transaction occurs.

5. Ensure that employees involved in the online banking process receive adequate internet security awareness training.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

The District officials' response to this audit can be found on the following page.

BLOOMFIELD
CENTRAL SCHOOL DISTRICT

Michael Midey, SUPERINTENDENT OF SCHOOLS

45 MAPLE AVENUE, SUITE A, BLOOMFIELD, NY 14469 p: (585) 657-6121 EXT. 4004 f: (585) 657-6060 WWW.BLOOMFIELDCSD.ORG

April 20, 2016

This letter serves as the Bloomfield Central School District's response to the most recent audit conducted by the Office of the State Comptroller. The District would like to note that we appreciate the time spent by the representatives of the Comptroller's Office reviewing our online banking procedures and explaining the findings of their audit. We value the information and the recommendations that, when fully implemented, will add an additional level of security to our online banking transactions.

The Bloomfield Central School District agrees with the recommendations in the report and is currently taking steps to correct any concerns. Corrective action will be completed by July 1, 2016.

Sincerely,

Michael J. Midey, Superintendent

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

To achieve our audit objective and obtain valid evidence, we performed the following procedures:

- We interviewed District officials to obtain an understanding of the District's online banking practices.
- We reviewed District policies to determine if the Board has adopted adequate online banking policies.
- We observed online banking user access from log-on to log-off.
- We inquired about written agreements with banks and online banking and wire transfer procedures.
- We examined the two District computers used to access online banking.
- We reviewed all online banking transactions for one month to determine if they were appropriate. We selected the most recently completed month which was September 2015.

We conducted this performance audit in accordance with 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.

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
http://www.osc.state.ny.us/localgov/

APPENDIX D

OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller
Tracey Hitchen Boyd, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BINGHAMTON REGIONAL OFFICE
H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins Counties

BUFFALO REGIONAL OFFICE
Jeffrey D. Mazula, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming Counties

GLENS FALLS REGIONAL OFFICE
Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

Serving: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington Counties

HAUPPAUGE REGIONAL OFFICE
Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE
Tenneh Blamah, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester Counties

ROCHESTER REGIONAL OFFICE
Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

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

SYRACUSE REGIONAL OFFICE
Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence Counties

STATEWIDE AUDITS
Ann C. Singer, Chief Examiner
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313