OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

York Central School District

Online Banking

Report of Examination

Period Covered:

July 1, 2014 – August 5, 2016

2016M-295

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

November 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 York 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 York Central School District (District) is located in the Towns of Leicester and York in Livingston County and the Town of Perry in Wyoming 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 day-to-day management of the District under the Board's direction. The Treasurer is responsible for performing online banking transactions and the Business Administrator[1] oversees the District's use of online banking.

The District operates an elementary school and a combined middle/high school on one campus with approximately 735 students and 165 employees. The District's budgeted appropriations for the 2016-17 fiscal year are $16.8 million, funded primarily with State aid and real property taxes.

The District uses network resources for performing online banking transactions. The District's Information Technology Coordinator 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 whether the District's 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 August 5, 2016. 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 our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such

[1] The Business Administrator referred to in this report left the District as of June 30, 2016. His replacement started on July 18, 2016.

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 initiate 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 funds held in the District's 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 are allowed to disburse or transfer funds in their custody by means of electronic or wire transfer. Because wire transfers of funds typically involve significant amounts of money, the District must control the processing of its wire transfers to help prevent unauthorized transfers from occurring. It is essential that District officials establish procedures and provide training to ensure that staff are securely accessing banking websites to help reduce the risk of unauthorized transfers from both internal and external sources.

Although the District's policy indicates that it has a written online banking agreement with its bank, District officials were not aware of any agreements regarding online banking. The Board adopted an online banking policy, but District officials did not develop written procedures for online banking activities. District officials also did not adequately segregate online banking duties and did not dedicate a separate computer for online transactions to limit access to online bank accounts. Furthermore, both the Treasurer and Business Administrator have the ability to perform online banking transactions, but neither has received Internet security awareness training. As a result, there is an increased risk that inappropriate transactions or misappropriations could occur.

Bank Agreement

General Municipal Law (GML) 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 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 that of the initiating entity and detecting errors in transmission or content of the payment order.

The District has one bank that it uses for online transactions that include electronic and external wire transfers and automated clearing house (ACH) payments.[2] Although the District's policy indicates that

[2] The Automated Clearing House is an electronic network used to process large volumes of electronic payments between banks. The District generally uses ACH payments for payroll.

it has a written agreement with the bank, it did not have a copy of the two agreements for wire funds transfers and ACH transactions onsite. District officials were not aware of these agreements and had to contact the bank to get copies. Our review of the agreements found they did not address any other electronic transfers, such as transfers between District accounts performed through the online banking website. Further, all accounts used for transfers were not included in the agreements. Although both agreements identified the authorized District users and detailed the security procedures to be used, the ACH agreement did not list the Treasurer as an authorized user for ACH transactions.

Without an adequate banking agreement, District officials cannot be assured that funds are effectively safeguarded during online transactions.

Policies and Procedures

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

The Board adopted an online banking policy that assigns the Business Administrator the responsibility of authorizing online banking transactions and the Treasurer the authority to process online banking transactions. The policy also authorizes the deputy Treasurer, who is the Business Administrator, to perform online banking transactions in the Treasurer's absence. Additionally, the policy requires the involvement of at least two individuals in each transaction and the creation of procedures that specifiy who is authorized to initiate, approve, transmit, record, review and reconcile electronic transactions. Finally, the policy requires the preparation of a monthly report detailing all online banking activity for review by staff independent of the online banking process and reconciled with the bank statement. However, District officials did not develop procedures, two individuals were not involved in each transaction and neither the Business Administrator nor the Treasurer prepared a monthly report of online banking activities for independent review and reconciliation.

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 that segregate job duties help ensure that employees are unable to perform financial transactions unilaterally. Requiring a second authorization or notification for completed transfers and

changes to the established transfer limits provides an added level of security over online transactions. A good detective control would be to require banks to provide emails to District officials alerting them every time an online transaction occurs. District officials could also provide for an independent review of bank reconciliations to detect and address unauthorized transfers after they have occurred.

The District has not adequately segregated employee duties for online banking. The Treasurer and Business Administrator had full access to the bank accounts and the bank did not send notifications every time an online transaction occurred. As a result, the Treasurer and Business Administrator were allowed to make transfers to and from District bank accounts and make ACH transactions without the review or authorization of any other District employee or official. However, the Business Administrator told us he did not know how to perform a transfer in the online banking website and only accessed it to review bank account balances. Instead, he initiated external wire transfers by a fax, which only requires one signature. The Business Administrator can also unilaterally change the daily transfer limit with the Bank without confirmation or notification sent to another District official.

Although the policy requires an independent review and reconciliation of bank statements, the Business Administrator receives the bank statements from the bank and reviews them prior to providing them to the Treasurer, who performs bank account reconciliations. Therefore, there is only a very limited control to help identify inappropriate activity. Furthermore, inappropriate transactions could go undetected for longer than necessary because there is about a month between these reviews and because more than a month of online banking activity has elapsed when the reviews occur.

Authorized Access

Good management practices would not only limit the users authorized to execute online banking activities but would 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,[3] which can threaten online bank accounts.

[3] Phishing attacks use fake email messages pretending to represent banks. The emails request information such as names, passwords and account numbers and provide links to fake websites.

District officials can also purchase computer fraud and funds transfer insurance coverage to help recoup a portion of funds misappropriated through computer fraud.

The District did not ensure that authorized access to the District's online bank accounts was limited because it did not dedicate a separate computer just for these transactions. In addition, both the Treasurer and Business Administrator accessed the online banking website, but neither has received Internet security awareness training. This could result in users unintentionally exposing the District's online bank accounts to malicious software, which could endanger District assets. We reviewed two months' of non-check, online banking wire transfers and ACH transactions and found that all 36 transactions were for appropriate District purposes.[4]

We recognize that 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. However, dedicating a computer for online banking and providing Internet security training for those involved in online transactions can help reduce the District's risk of funds being misappropriated due to unauthorized access.

Recommendations

District officials should:

1. Ensure there are sufficient written agreements with any banks and those who perform online banking transactions are familiar with their content. Such agreements should address electronic transfers, include all accounts used for transfers and list the Treasurer as an authorized user for ACH transactions.

2. Establish written online banking procedures as specified in the Board policy that adequately segregate duties and require independent verification of transfers. The procedures should also require the preparation of a monthly report detailing all online banking activity for review by staff independent of the online banking process and reconciled with the bank statement.

3. Enable notifications and other security measures available from the District's bank, including email notifications that advise the Treasurer and Business Administrator every time an online transaction or fax occurs.

[4] Refer to Appendix B for information on sample selection.

4. Require secondary authorization for increases to daily transfer limits.

5. Designate a computer to be used only for online banking transactions.

6. 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.

York Central School

Dr. Daniel P. Murray, *Superintendent*

William R. McDonald, *Business Administrator*

Lindsey M. Peet, *Director of Curriculum & Instruction*

GOLDEN KNIGHTS

David J. Sylvester, *Middle/High School Principal*

Mary Kate Noble, *Elementary Principal*

Svetlana D. Stowell, *Pupil Personnel Services Director*

November 7, 2016

Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
Rochester Regional Office
The Powers Building
16 West Main Street, Suite 522
Rochester, New York 14614-1608

Dear Mr. Grant,

We received the preliminary draft findings report from your most recent audit (covering the time period July 1, 2014 through August 5, 2016). This audit focused on online banking, specifically looking to ascertain if our online banking transactions were safeguarded. We have shared this draft report with our Board of Education and appropriate district administrators. We are in agreement with your findings and will work on a corrective action plan. Your recommendations will be very helpful as we strive to maintain the highest level of security for our electronic transactions.

Thank you.

Sincerely,

Daniel P. Murray
Superintendent of Schools

PO BOX 102 • 2578 Genesee Street • Retsof, NY 14539 • Phone: 585-243-1730 • Fax: 585-243-5269 • www.yorkcsd.org

Providing quality education where children come first.

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 regarding online banking and electronic transfers.

- We inquired about written agreements with banks and online banking and wire transfer procedures. We reviewed the written agreements acquired from the bank.

- We examined the two District computers used to access online banking.

- We reviewed all non-check transactions for two months to determine whether they were appropriate District expenditures. We selected the two most recently completed months prior to the beginning of our fieldwork, which were April and May 2016.

- We reviewed the District's insurance policy for computer fraud and funds transfer insurance coverage.

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