OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Byron-Bergen Central School District

Online Banking and Information Technology

Report of Examination

Period Covered:

July 1, 2013 — June 6, 2014

2014M-261

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

December 2014

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 operations and Board of Education governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard district assets.

Following is a report of our audit of the Byron-Bergen Central School District, entitled Online Banking and Information Technology. 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 Byron-Bergen Central School District (District) is located in the Towns of Byron and Bergen in Genesee County. The District is governed by a Board of Education (Board), which comprises 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 (Superintendent) 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 School Business Official (Business Official) is responsible for accounting for the District's finances, maintaining accounting records and preparing financial reports.

The District has two schools in operation, with an enrollment of approximately 1,040 students. The District's budgeted appropriations for the 2014-15 fiscal year total $21.3 million and are funded primarily with real property taxes and State aid.

The District uses network and web resources to support certain business operations, such as performing online banking transactions and maintaining personal, private and sensitive information including student records. The District's Information Technology Support Specialist 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 evaluate internal controls related to online banking and information technology (IT). Our audit addressed the following related question:

- Did the Board and District officials establish effective online banking internal controls to ensure adequate protection of the District's assets and to identify security vulnerabilities in the District's website and internal network?

Scope and Methodology

We examined the District's online banking practices for the period July 1, 2013 through June 6, 2014. We also examined IT controls over certain District functions. Our audit disclosed areas in need of improvement concerning these IT controls. Because of the sensitivity of this information, certain vulnerabilities are not discussed in this report but have been communicated confidentially to District officials so they could take corrective action.

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 is included in Appendix C of this report.

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 the findings and recommendations and indicated they would take certain corrective action. Appendix B includes our comment on an issue raised in the District's response letter.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of the New York State General Municipal Law, Section 2116-a (3)(c) of the New York State Education Law and Section 170.12 of the New York State 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 allows the convenience of moving money between bank accounts, reviewing transaction histories, reconciling accounts at any time and closely monitoring cash balances for more effective management. School districts are allowed to disburse or transfer funds in their custody by means of electronic or wire transfer.[1] However, since connecting to the Internet is a necessary part of the online banking process, a multitude of vulnerabilities must be recognized and anticipated. Although online banking fraud is often committed by external parties, risks posed by internal employees must also be considered. The ease and speed at which large amounts of money can be transferred among accounts pose great potential risks. Poor controls over online banking increase the risk that an entity may become the victim of cyber fraud and experience financial losses that may not be recoverable.

The tactics used to commit fraud can range dramatically in sophistication and continually evolve over time. A best practice for protecting IT systems, information and local government resources is to build successive layers of defense mechanisms. District officials are responsible for establishing effective controls to reduce online banking risks to acceptable levels through a combination of different controls.

We reviewed the District's online banking practices and found that the Board and District officials did not establish adequate online banking internal controls to ensure sufficient protection of the District's assets. We identified areas that need to be improved to reduce the inherent risks of online banking. The District unnecessarily has online banking access for all of its bank accounts.[2] In addition, District officials do not secure user names, passwords and secured tokens.[3] They also do not consistently erase the browser history after online banking. Further, the District did not have agreements with its banks to clearly prescribe the manner in which electronic or wire transfer of funds would be accomplished. District officials also have not enabled necessary alerts and other security measures available from the District's banks.

Number of Bank Accounts – The District uses two banks and has online banking capability for all of its bank accounts. Reducing the number

[1] Per General Municipal Law

[2] Because of the sensitivity of this information, we are not disclosing the number of bank accounts.

[3] A secured token is a small electronic device that dynamically generates a code.

of accounts used for online banking, especially savings accounts with high balances, reduces risk. We discussed our concerns with specific bank accounts with District officials and are not disclosing them in this report due to security concerns.

User Credentials − Credentials such as user name, password and secured token are needed to access online banking and used to identify a particular online banking user. Those credentials should be properly secured. Three employees have access to online banking using their own separate unique user name, password and secured token. However, two of these employees (the Clerk and Treasurer) wrote down their user names and passwords and keep the information with their secured token in two file cabinets. Other District employees have access to one of these file cabinets and the other is often unlocked, which increases the risk that their user information could be accessed by others and used inappropriately.

Terminating Online Banking Sessions − It is important to completely log off from Internet banking sessions; simply closing the web browser window that the transaction was performed in may not terminate the banking session. District employees do not log off the bank's website in a secure manner after an online banking session. If the computers used for online banking became infected with a malicious program, a user's session could be hijacked and financial transactions could be performed without his or her knowledge. It is crucial to erase the web browser cache, temporary Internet files, form data, cookies and history after an online banking session is completed. Erased information thereby would not be on the system to be stolen if the system was compromised by a hacker or malware program. The Business Official and the Clerk do not erase the web browser cache, temporary Internet files, cookies and history after an online banking session. The Treasurer stated that she may erase them every three to four months.

Banking Agreements − General Municipal Law requires a government entity to enter into a written agreement with banks. The agreement should prescribe the manner in which electronic or wire transfers of funds will be accomplished, including who is authorized to make transfers and from which bank accounts. The District does not have such an agreement in place with either bank.

Transfer Verification − A good process for verifying the authenticity of requested wire transfers is critical to reduce the risk of fraudulent transfers. Requiring call backs is an effective preventive control, while advisories alerting that transfers have occurred can be a good detective control. For electronic and wire transfers at both of the District's banks, no one person can complete a transaction. One individual inputs the request and a second employee needs to sign in

to release it. However, only one bank alerts the District by sending an email to the Business Official and a letter to the Superintendent to inform them of an electronic transfer (internal and external) or wire transfer. For wire transfers, the bank also performs callbacks to the releaser to confirm the transfers. However, the other bank does not have those measures in place. Furthermore, the District does not need to transfer money to a foreign country. However, District officials did not ensure that the banks automatically blocked wire transfers to foreign countries.[4] Automatically blocking foreign transfers would reduce the potential, unnecessary risk.

During the audit, we also examined the three computers used for online banking and reviewed the District's internet network and public website to assess their security vulnerabilities. We communicated the results of those tests to District officials separately and confidentially due to security concerns.

Recommendations

The Board and District officials should:

1. Consider limiting the online banking capability to certain accounts.

2. Ensure that all online banking users effectively secure the credentials used to access online banking.

3. Ensure that online banking users log off a bank's website in a secured manner by completely logging off from Internet banking sessions and erasing the web browser cache, temporary Internet files, form data, cookies and history after an online banking session is complete.

4. Have written agreements with banks prescribing the manner in which electronic or wire transfers of funds will be accomplished, identifying the names and numbers of the accounts from which electronic or wire transfers may be made and identifying which individuals are authorized to request an electronic or wire transfer of funds.

5. Ensure that alerts and other security measures available from the banks are enabled. Such measures could include, but are not limited to:

   - Call back verifications for certain transactions.
   - An alert system that advises District officials by email or text every time an online transaction occurs.
   - Automatically blocking wire transfers to foreign countries.

[4] One bank automatically blocked foreign transfers during our audit.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

BYRON-BERGEN CENTRAL SCHOOL DISTRICT
District Office
6917 West Bergen Road
Bergen, NY 14416-9747
(585) 494-1220
FAX (585) 494-2613

Superintendent – Casey Kosiorek
Business Official – William E. Snyder, Jr.
Special Education Chairperson – Donna M. Moscicki, Ed.D.

October 30, 2014

Jeffrey D. Mazula, Chief Examiner
Buffalo Regional Office
New York State Comptroller
295 Main Street, Room 1050
Buffalo, New York 14203-2510

Dear Mr. Mazula,

On behalf of the Byron-Bergen Central School District I hereby acknowledge receipt of the *Byron-Bergen Central School District Online Banking and Information Technology Report of Examination* – in draft form for the period of July 1, 2013 to June 6, 2014. This letter shall serve as our official response and corrective action plan.

We have thoroughly reviewed the draft report and the District is committed to ensuring that we are being fiscally responsible in safeguarding against unauthorized access of district funds through online banking.

Recommendation 1: Consider limiting the online banking capability to certain accounts.

District Response/Corrective Action: Due to the remote location of our school district and limited district office staff due to the ever increasing budget constraints caused by the property tax cap, freezing of state aid and the Gap Elimination Adjustment, we are unable to do banking transaction on a regular basis at our banking institutions' branch locations due to distance and time away from other duties district office staff perform. We must be as efficient as possible in the use of our existing office staff. That efficiency is increased with the ability to do our banking functions online. These online banking procedures are limited to certain personnel completing different steps in the processes providing necessary internal controls for safeguarding district assets.

Recommendation 2: Ensure that all online banking users effectively secure the credentials to access online banking.

District Response/Corrective Action: All online banking users understand the need to safeguard their credentials to prevent unauthorized online access to banking information. Each user will continue to secure their credentials in a manner necessary to ensure their safety. Additional steps have been put in place to ensure that each individual's credentials are under lock and key when not in use.

Recommendation 3: Ensure online banking users log off the bank website in a secure manner by completely logging off the Internet banking sessions and erasing the web browser cache temporary Internet files, form data, cookies and history after an online banking session is completed.

District Response/Corrective Action: Upgrades have been made to all online banking users' operating systems. Training has been provided to instruct users on the proper procedures to follow when terminating an online banking session.

Recommendation 4: Have a written agreement with banks prescribing the manner in which electronic or wire transfer of funds will be accomplished; identifying the names and numbers of the accounts from which electronic or wire transfers may be made; and identifying which individuals are authorized to request an electronic or wire transfer of funds.

District Response/Corrective Action: The District has written banking agreements in place with all institutions where district funds are deposited. These agreements outline the entire banking relationship between the District and the banking institution up to and including online banking procedures. The District, however, elects to not maintain any written documents on its premises that give specific information as to the manner in which electronic or wire transfer of funds will be accomplished other than instructional manuels, identification of the names and numbers of the bank accounts that said transfer may be made from or identify the individuals who are authorized to make said transfers. The District believes that this information should be housed with the banking institution and changed only when authorized by the Board of Education. This information is vital to the safety of the District's assets and is therefore safer with the banking institutions.

See Note 1 Page 11

Recommendation 5: Ensure that alerts and other security measures from the bank are enabled. Such measures could include, but not limited to:

a. Call back verifications for certain transactions
b. An alert system that advises District officials by email or text every time an online transaction occurs.
c. Automatically blocking wire transfer to foreign countries.

District Response/Action Plan: The District has reviewed the alert systems that are currently available by its banking institutions to ascertain all features necessary to safeguard district assets are activated. Many of those safeguards have been and will continue to be in place. The banking institutions' services currently utilized are deemed to be adequate and do not cost the District any additional banking fees. Additionally, all notices that are currently received via email for online activities are printed and kept on file with the monthly cash receipts records. In certain instances the banking institutions mail confirmation notices to the Superintendent of Schools which are signed off on and matched to previously retained notifications.

The feature allowing for wire transfers to foreign countries was cancelled immediately upon realization it was active. This service was never intended to be available to district employees and should not have been activated by the banking institutions. We are grateful that this was diagnosed in the audit.

It is important to the District to ensure, during these difficult budget times, that unnecessary expenditure/diversion of funds away from the educational program needs is avoided at all times. Some of the security services offered by the banking institutions require a bank charge and in many cases is a duplication of a control that is already in place. The District cannot justify expending funds for these services.

The Byron-Bergen Central School District would like to thank the audit team for their review of our online banking procedures. The audit team members were professional and courteous to our district staff throughout the examination period. We will continue to self- monitor our online procedures to ensure we are safeguarding the District's assets in the best way possible at all times.

Sincerely,

~~Debra List~~ Daniel P. Ireland
Vice- President – Board of Education

Casey Kosiorek
Superintendent of Schools

APPENDIX B

OSC COMMENT ON THE DISTRICT'S RESPONSE

Note 1

During our exit conference, District officials provided us an agreement with one of its two banks. However, the agreement did not contain specific and necessary information concerning electronic or wire transfers. We further question what benefits an agreement provides if it is not kept at the District and its content is not known to District officials and employees. District officials could find a safe way to keep its banking agreement at the District's premises. For example, District officials could maintain an electronic copy that could be encrypted and/or protected with a password.

APPENDIX C

AUDIT METHODOLOGY AND STANDARDS

Our objective was to assess the District's controls over online banking and information technology. To accomplish our objective, we performed the following procedures:

- We interviewed District officials to obtain an understanding of the District's online banking practices.
- We observed online banking users access online banking from log on to log off.
- We inquired about written agreements with banks and fund and wire transfer procedures.
- We examined three computers used to access online banking.
- We audited the District's internet network and public website to assess its security vulnerabilities.

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 D

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 E

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

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller
Nathaalie N. Carey, 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