



Caledonia-Mumford Central School District Online Banking

Report of Examination

Period Covered:

July 1, 2014 – June 30, 2016

2016M-227



Thomas P. DiNapoli

Table of Contents

	Page
AUTHORITY LETTER	1
INTRODUCTION	2
Background	2
Objective	2
Scope and Methodology	2
Comments of District Officials and Corrective Action	3
ONLINE BANKING	4
Bank Agreement	4
Segregation of Duties	5
Authorized Access	6
Recommendations	7
APPENDIX A Response From District Officials	8
APPENDIX B Audit Methodology and Standards	10
APPENDIX C How to Obtain Additional Copies of the Report	11
APPENDIX D Local Regional Office Listing	12

State of New York Office of the State Comptroller

Division of Local Government and School Accountability

October 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 Caledonia-Mumford 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 Caledonia-Mumford Central School District (District) is located in the Town of LeRoy in Genesee County, the Town of Caledonia in Livingston County and the Towns of Chili, Riga and Wheatland in Monroe County. The District is governed by the Board of Education (Board) that 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 Treasurer is responsible for completing banking transactions, and the District Business Manager is responsible for overseeing these transactions.

The District operates three schools on one campus with approximately 820 students and 165 employees. The District's budgeted appropriations for the 2016-17 fiscal year are \$17.1 million, which are 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 June 30, 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 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.

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 provide authorization of 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.

Although the District's policy indicates that it has a written online banking agreement with its bank, District officials told us they do not have an agreement with the bank. They 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 Manager perform online banking transactions, but neither has received Internet security awareness training.

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.¹ Although the District's policy indicates that it has a written agreement with the bank, it did not have a copy of the agreement onsite. Also, District officials told us that they do not have an agreement with the bank. The District has a few bank documents

¹ 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.

that provide information on the capabilities for performing electronic funds transfers, such as describing the dollar limit for the amount of electronic payments. However, these documents are limited in that they do not identify the bank account numbers, names of authorized District users for online banking or other details that should be included in a written agreement.

The District has established some security controls with the bank for online banking, such as secondary authorizations for wire transfers and ACH debits. However, there are no notifications or alerts sent for transfers between District accounts. Also, while the bank sends the Treasurer email notifications after it completes wire transfers, the Business Manager told us that he does not receive any notifications.

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

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 Board adopted an online banking policy that requires at least two individuals be involved in each transaction. Also, District officials developed regulations stating that one person should initiate wire, ACH and other electronic transfers and a second individual should release the funds. However, we found that two individuals are not involved in each transaction, and the District has not adequately segregated employee duties related to online banking transactions.

The Treasurer has access to all of the District's bank accounts, which enables her to make transfers to and from District bank accounts² without the review or authorization of another District official. The bank does not send any notifications to District officials for these transactions. Although the Treasurer initiates and the Business Manager authorizes external wire transfers and ACH payments, we

² The District uses more than one bank and makes ACH or wire transfers between accounts at these separate banks.

found that the bank does not send a confirmation of the transfers to both officials. Additionally, the Treasurer can increase the daily transfer limit without the Business Manager's approval, and the bank does not notify the Business Manager when the daily limit has been increased.

The Treasurer prepares an online banking transfer log for the month and provides it to the Business Manager at the end of the month for use in recording certain transfers and reviewing bank statements. The Business Manager receives the District's bank statements from the bank and reviews them prior to providing them to the Treasurer, who performs bank account reconciliations. 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 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 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. Computer users' visitation of personal or nonbusiness sites heightens this risk. 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. Although the District's regulations state that, if possible, the business office and/or Treasurer should designate a specific computer for online banking, the Treasurer told us she did not know who would be responsible for making this decision. Also, the Business Manager told us that this option had not been discussed recently. Further, the Treasurer and Business Manager's use of their District computers for personal and nonbusiness purposes and online banking activities could make the District more susceptible to unauthorized access.

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.

In addition, both the Treasurer and Business Manager perform online banking transactions, but neither has received Internet security awareness training. 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. We reviewed two months of online banking and wire transfers and ACH transactions and found that all 54 transactions made during this time 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 that the District has a sufficient written agreement with the bank and that those who perform online banking transactions are familiar with its content.
2. Enable notifications and other security measures available from the District's bank, including email notifications that advise the Treasurer and Business Manager every time an online transaction occurs.
3. Require secondary authorization for increases to daily transfer limits.
4. Designate a computer to be used only for online banking transactions.
5. Ensure that employees involved in the online banking process receive adequate Internet security awareness training.
6. Monitor computer usage to ensure compliance with the District's acceptable use policy and regulations.

⁴ Refer to Appendix B for further information on our sample selection.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

CALEDONIA-MUMFORD CENTRAL SCHOOL

99 NORTH STREET
CALEDONIA, NEW YORK 14423



District Office (585) 538-3400
Elementary School (585) 538-3481
Middle School (585) 538-3482

High School (585) 538-3483
Special Education (585) 538-3404
Guidance Office (585) 538-3445

October 11, 2016

Mr. Edward V. Grant Jr.
Chief Examiner
The Powers Building
16 Main Street Suite 522
Rochester NY 14614-1608

Dear Mr. Grant:

This letter serves as the Caledonia-Mumford Central School District's official response to the DRAFT Report of Examination-Online Banking for the period of July 1, 2014 - June 30, 2016 issued by the NYS Office of the State Comptroller.

The Caledonia-Mumford Central School District greatly appreciates the time taken by the examiners and the professionalism shown throughout the audit process. The Caledonia-Mumford Central School District accepts this audit and views this report as an important tool in maintaining a high level of accountability to our stakeholders.

The District appreciates the comprehensive and thorough review of our online banking practices and has already initiated a corrective action plan to address identified recommendations in order to safeguard financial information.

The District continues to demonstrate great pride in our work and will continue to review our practices to maintain appropriate controls and accountability over financial operations.

Sincerely,

A handwritten signature in black ink, appearing to read 'John Bickford', written over a faint circular stamp.

John Bickford
School Board President

cc: Robert Molisani, Superintendent
Patrick Donegan, Business Manager
Board of Education

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 and regulations for online banking and electronic transfers.
- We observed online banking user access from logon to logoff.
- We inquired about written agreements with banks and online banking and wire transfer procedures. We reviewed the limited documentation available from the bank regarding capabilities for electronic transfers.
- We examined the two District computers used to access 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 prior to the beginning of our fieldwork, which were February and March 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,
Osego, 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-Bufferalo@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