

MARCELLUS CENTRAL SCHOOL DISTRICT

2 REED PARKWAY, MARCELLUS, NY 13108
(315) 673-6000
marcellusschools.org

MICHELLE L. BRANTNER
Superintendent
315-673-6000

ANTHONY J. SONNACCHIO
School Business Administrator
315-673-6001

September 14, 2020

Office of the State Comptroller
Division of Local Government & School Accountability
PSU – CAP Submission
110 State Street, 12th Floor
Albany, NY 12236

New York State Education Department
Office of Audit Services, Room 524 EB
89 Washington Avenue
Albany, NY 12234

Unit Name: Marcellus Central School District
Audit Report Title: Online Banking
Audit Report Number: 2020M-66

To Whom It May Concern:

For each recommendation included in the audit report for the Marcellus Central School District, the following are our corrective actions to be taken or proposed.

Audit Recommendation

The audit process identified findings related to the district's online banking policy. Key findings relate to the need to improve monitoring procedures, require confirmation from the district's banks for all electronic transactions, and to clearly indicate in the policy how online transactions are to be authorized and processed.

Implementation Plan of Action

The District will update its online banking policy to clearly describe the procedures for authorizing and processing transactions.

Implementation Date

November 2020

Person Responsible

School Business Administrator

Audit Recommendation

The audit process identified a need to ensure that a dedicated computer is used to perform online transactions, and that employees involved in online banking receive internet security awareness training.

Implementation Plan of Action

The District will install and use separate Chromebox devices to serve as dedicated computers for use in performing online transactions. The District will provide internet security awareness training for all employees involved in online banking.

Implementation Date

February/June 2020

Person Responsible

School Business Administrator

If you have any questions or require additional information, please feel free to contact me.

Sincerely,



Michelle Brantner
Superintendent of Schools

Marcellus Central School District

Online Banking

SEPTEMBER 2020



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

Contents

- Report Highlights 1**

- Online Banking 2**
 - How Should Officials Safeguard Online Banking Transactions?. . . . 2
 - Officials Should Improve Controls Over Online Banking Transactions 3
 - A Dedicated Computer Was Not Always Used for Online Banking
and Internet Security Training Was Not Provided 3
 - Officials Entered Into Online Banking Agreements But Did Not
Always Require Confirmations. 4
 - What Do We Recommend? 5

- Appendix A – Response From District Officials 6**

- Appendix B – Audit Methodology and Standards 7**

- Appendix C – Resources and Services 9**

Report Highlights

Marcellus Central School District

Audit Objective

Determine whether District officials established controls to ensure online banking transactions were appropriate and secure.

Key Findings

- Officials segregated the duties of employees responsible for online banking transactions, but they could further strengthen controls by improving their monitoring procedures.
- Officials entered into agreements with the District's banks, but did not require confirmations for all electronic transactions.
- The online banking policy does not clearly indicate how online transfers will be authorized and processed.
- A dedicated computer was not always used for online banking and none of the employees involved in online banking received Internet security awareness training.

Key Recommendations

- Update the online banking policy to clearly describe the procedures for authorizing and processing transactions.
- Ensure that a dedicated computer is used to perform online transactions and that employees involved in online banking receive Internet security awareness training.

District officials agreed with our recommendations and indicated they planned to initiate corrective action.

Background

The Marcellus Central School District (District) serves the Towns of Marcellus, Camillus, Onondaga, Otisco, Skaneateles, and Spafford in Onondaga County.

The District is governed by a Board of Education (Board) composed of seven elected members. The Board is responsible for the general management and control of District 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 Treasurer and Deputy Treasurer are responsible for online banking transactions, and the Business Administrator is responsible for overseeing these transactions.

Quick Facts

Employees	312
2019-20 Appropriations	\$38 million
Online Banking July 1, 2018 – October 31, 2019	
Transactions	571
Transactions Amount	\$110 million

Audit Period

July 1, 2018 – October 31, 2019

Online Banking

Online banking provides a way to directly access funds in district bank accounts. Users can review current account balances and information, including recent transactions, and transfer money between District accounts or to external accounts. New York State General Municipal Law (GML)¹ allows school districts to disburse or transfer funds in their custody by electronic or wire transfers.

How Should Officials Safeguard Online Banking Transactions?

The school board should adopt a comprehensive written online banking policy (Policy) and periodically review and update it. The Policy should at a minimum:

- Clearly describe the online activities District officials may perform,
- Specify which employees are authorized to process transactions,
- Establish an approval process to verify the accuracy and legitimacy of transfer requests, and
- Require the review and reconciliation of transfers.

Officials should segregate the duties of employees granted access to online banking. Employees should be assigned unique usernames and passwords that are not shared with other users, and advanced authentication techniques (i.e., two-factor authentication with a password and security question or personal identification number) should be used to log into the online banking platform. Bank accounts should be monitored at least every two or three days and regular, independent reviews of bank statements and supporting documentation should be performed to help detect any unauthorized or suspicious activity.

A school district's banking agreements should prescribe the manner in which transfers can be made. It should identify individuals authorized to make online transfers and which bank accounts can be used for online transfers. The agreement should also include security procedures designed to ensure payment orders are legitimate and that can detect transmission or content errors. The bank should be required to provide written confirmation when funds are transmitted.

Officials also should limit the number of users and computers authorized to conduct online banking. To minimize exposure to malicious software, authorized users should access bank accounts only from a dedicated computer connected through a wired network. Finally, employees with online banking access should receive Internet security awareness training to educate them on safe computing practices.

Employees with online banking access should receive Internet security awareness training.

¹ General Municipal Law Section 5-A

Officials Should Improve Controls Over Online Banking Transactions

We reviewed 352 online banking transactions totaling \$89.4 million that were processed during the audit period and found they were all for appropriate purposes. While we also found online banking responsibilities for initiating and approving online transactions were segregated and advanced authentication techniques are required to conduct online banking, officials should improve the District's monitoring procedures for online banking and update the District's online banking policy.

Monitoring of Transactions – Although the District's tax collector completes monthly bank reconciliations, no one compares external bank transfers reflected on the bank statements to the supporting documentation, which would help identify any unauthorized or suspicious activity. In addition, the online banking transactions are not monitored timely. The Treasurer told us she does a cursory review of bank balances and transactions whenever she logs into the online banking platforms to initiate transfers; however, this is not a consistent review and therefore may not identify inappropriate transactions in a timely manner.

Online Banking Policy – The Board's online banking policy, last revised on November 16, 2010, has not been reviewed or updated to include the District's current online banking procedures. It identifies individuals authorized to perform online banking transactions and generally describes the online activities officials may perform. It also requires a review and reconciliation of electronic or wire transfers to the bank statements. However, it does not clearly convey specific procedures or how online transfers will be approved. For example, it does not specify how approval will be granted or documented or whether some or all types of electronic transfers require approval. The policy also states: "The Internal Auditor will periodically confirm that wire transfers have appropriate signatures, verification and authorization of proper personnel." However, the District does not have an internal auditor to perform this review and this responsibility was not assigned to someone else. In addition, wire transfers do not require signatures to document approval. Finally, although the District's agreements with its two banks provide for compensating controls, the policy does not limit the number of individuals authorized to add new bank accounts as external transfer options for all District bank accounts.

A Dedicated Computer Was Not Always Used for Online Banking and Internet Security Training Was Not Provided

While the Treasurer has a District computer dedicated for online banking transactions, she and other designated officials can use their assigned District computers to conduct online banking. These computers are used for non-banking purposes.

We reviewed the website browsing history on the dedicated computer and the computers of the Treasurer, Deputy Treasurer and Business Administrator to determine whether any employees had visited websites other than those necessary to conduct online banking. Although the dedicated computer was only used for online banking purposes, the other three computers were used for email and for accessing various websites. Online banking transactions should be limited to a dedicated computer(s), as this practice can help minimize a system compromise.

We also found that Internet security awareness training was not provided to the Treasurer, Deputy Treasurer or Business Administrator. Officials told us all District employees are emailed throughout the year to inform them of potential noteworthy cybersecurity risks, but no formal security awareness training is provided.

Using the same computers for online banking and non-online banking activities – combined with the lack of Internet security training – increases the risk that users could unintentionally expose online bank accounts to threats from malicious software and place District cash assets at risk.

Officials Entered Into Online Banking Agreements But Did Not Always Require Confirmations

The District maintains accounts with online transfer capabilities at two banks and has a written agreement with each to define the terms and conditions for online banking. The agreements also establish access and control settings within the online banking platforms that prescribe how electronic and wire transfers will be accomplished, identify the names and numbers of the accounts from which transfers may be made and identify the individuals authorized to request transfers. In addition, security procedures have been implemented for accounts at the banks to prevent and detect unauthorized external transfers. However, the bank agreements do not require the banks to provide confirmations for all electronic transactions.

The agreement with one bank specifies that only individuals authorized to disburse District funds (District signatories) can add new bank accounts as an external transfer option. However, two users are required to execute an electronic (Automated Clearing House (ACH)² or wire) transfer to the new external bank account: one to initiate the transfer and a different user to approve and complete it. Both of these individuals receive an email from the bank to confirm that a wire transfer occurred, but no confirmation is sent for ACH transactions. In addition, the District provides the bank with employee names and IP addresses of computers authorized to access the bank accounts to conduct online banking transactions.

² An electronic funds transfer network that connects U.S. bank accounts

The other bank allows any individual with online banking access to add a new bank account as an external transfer option, but two separate users are required to initiate and approve the electronic or wire transfer. The District provides the bank with the names of employees authorized to access the accounts for online banking. However, this bank does not send an email or written confirmation of transmitted funds.

What Do We Recommend?

The Board should:

1. Update the online banking policy to clearly describe the procedures for authorizing, processing and reviewing online banking transactions.

District officials should:

2. Ensure that the reconciliation of transfers includes the review of supporting information for each external electronic and wire transaction, and that online banking activity is reviewed on a timely basis (every two to three days) to detect any unauthorized activity.
3. Limit the number of individuals authorized to add new bank accounts as external transfer options for all District bank accounts.
4. Amend the bank agreements to require the bank to provide written confirmation for all online banking activity once the requested funds have been transmitted.
5. Ensure that only a dedicated computer is used to perform online banking transactions.
6. Ensure that employees who are involved in the online banking process receive Internet security awareness training.

Appendix A: Response From District Officials

MARCELLUS CENTRAL SCHOOL DISTRICT

2 REED PARKWAY, MARCELLUS, NY 13108
(315) 673-6000
marcellusschools.org

MICHELLE L. BRANTNER
Superintendent
315-673-6000

ANTHONY J. SONNACCHIO
School Business Administrator
315-673-6001

July 9, 2020

Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
Syracuse Regional Office
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428

Dear Ms. Wilcox:

The Marcellus Central School District acknowledges receipt of a draft copy of the audit report entitled "Online Banking, Report of Examination 2020M-66". The District is in agreement with the recommendations made in the report and is in the process of amending policies and procedures to strengthen online banking procedures of the District. It is our intent to establish controls to ensure online banking transactions are appropriate and secure.

The district is implementing corrective actions to address recommendations made in the report:

- Update our online banking policy to clearly indicate how online transfers will be authorized and processed.
- Further strengthen controls by improving monitoring procedures and review of supporting information for online banking transactions.
- Limit the number of individuals authorized to add new bank accounts for external transfers.
- Request that banking institutions provide confirmations for all electronic transactions.
- Use a dedicated computer for online banking.
- Provide internet security awareness training for employees involved in online banking.

In closing, we would like to express our appreciation of the efforts of your office and the outcome of the audit process. If you have any questions or require additional information, please feel free to contact me.

Sincerely,



Michelle Brantner
Superintendent of Schools

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, we performed the following audit procedures:

- We interviewed District Officials to obtain an understanding of online banking practices and determine whether online banking users received Internet security training.
- We reviewed District policies and procedures to determine whether the Board adopted an adequate online banking policy.
- We reviewed the written agreements with banks and reviewed documentation regarding capabilities for electronic and wire transfers.
- We observed online banking user access from logon to logoff for the Treasurer and Deputy Treasurer.
- We examined the computers used to access online banking and reviewed their website browsing history.
- We identified 571 online banking transactions totaling \$109,550,460 during our audit period and examined 352 transactions (82 percent) totaling \$89,458,859. The 352 transactions consisted of all 309 intrabank transfers totaling \$59,109,250; all 19 intrabank and external wire transfers totaling \$28,428,690; and a randomly selected two months of 24 ACH payments totaling \$1,920,919 for payroll-related expenditures. We verified that all intrabank transfers were between District bank accounts, and reviewed supporting documentation for the external wire transfers and ACH payments to verify that the transactions were appropriate.

We conducted this performance audit in accordance with generally accepted government auditing standards (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.

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.

The Board has the responsibility to initiate corrective action. 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-a(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 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 CAP should be posted on the District's website for public review.

Appendix C: Resources and Services

Regional Office Directory

www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2018-12/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas

www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263196&issued=All

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems

www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management

www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263206&issued=All

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans

www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders

www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2020-05/cyber-security-guide.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/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers

www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263211&issued=All

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics

www.osc.state.ny.us/local-government/academy

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/local-government

Local Government and School Accountability Help Line: (866) 321-8503

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief Examiner

State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428

Tel (315) 428-4192 • Fax (315) 426-2119 • Email: Muni-Syracuse@osc.ny.gov

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



Like us on Facebook at facebook.com/nyscomptroller

Follow us on Twitter [@nyscomptroller](https://twitter.com/nyscomptroller)