REPORT OF EXAMINATION | 2022M-99

Mount Morris Central School District

Online Banking

NOVEMBER 2022

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

Contents

Report Highlights

Mount Morris Central School District

Audit Objective

Determine whether the Mount Morris Central School District (District) officials ensured online banking transactions were appropriate and secure.

Key Findings

While we found online banking transactions were appropriate, District officials did not secure access to online banking. In addition to sensitive information technology (IT) control weaknesses that we confidentially communicated to District officials, officials did not:

- Have an adequate written bank agreement for online banking transactions.
- Ensure that authorized access to online bank accounts was limited.
- Monitor computer use with the acceptable use policy and regulations.

Key Recommendations

- Ensure the written bank agreement sufficiently details online banking.
- Designate a computer for online banking transactions.
- Monitor computer use to ensure compliance with the acceptable use policy and regulations.

District officials generally agreed with our recommendations and indicated they will take corrective action. Appendix B includes our comments on certain issues raised in the District's response.

Background

The District serves the Towns of Mount Morris, West Sparta, Leicester and Groveland in Livingston County.

The District is governed by the Board of Education (Board), which is composed of seven elected members. The Superintendent of Schools (Superintendent) is the 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 Business Administrator is responsible for reviewing online banking transactions. The District Treasurer (Treasurer) initiates bank and wire transfers using online banking. District officials use network resources to perform online banking transactions. The Director of Facilities, Technology and Security is responsible for managing the network's security and the data it contains.

Quick Facts	
Bank balances as of February 28, 2022	$5.3 million
Online bank transfers completed and reviewed	$37.8 million
Wire transfers and Automated Clearing House payments reviewed	$2.8 million
Authorized online banking users	3

Audit Period

July 1, 2020 – May 18, 2022

Online Banking

New York State General Municipal Law (GML) Section 5-a allows school districts to disburse or electronically transfer funds, provided that the governing board has entered into a written agreement with the bank. This agreement must:

- 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 the initiating entity's and detecting errors in transmission or content of the payment order.

Online banking also provides a means of monitoring and accessing funds held in school district bank accounts. Users can transfer money between bank accounts and to external accounts and review account balances and account information.

How Can Officials Secure Online Banking and Reduce the Risk of Inappropriate Transactions?

School districts should control the online banking process to help prevent unauthorized transfers and inappropriate transactions from occurring. It is essential that school district officials authorize transfers before they are initiated and establish procedures to ensure that staff are securely accessing banking websites.

To safeguard cash assets, a school district board should adopt comprehensive written online banking policies and procedures and monitor and control online banking transactions. The policy should clearly describe the authorized online activities school district officials may engage in, specify who is authorized to process transactions, and establish a detailed approval process to verify the legitimacy and accuracy of transfer requests. School district officials should properly segregate the duties of employees who are granted access to the online banking applications to ensure that employees are unable to perform all phases of a financial transaction on their own. Someone independent of the online banking transactions must frequently monitor the activity to identify unauthorized or suspicious activity.

Good management practices should limit the number of users authorized to execute online banking activities, and authorized online banking users should access bank accounts from one computer (if possible) dedicated for online banking transactions. This will help minimize potential exposure to malicious software and other unauthorized access because a dedicated computer could have an isolated Internet connection, be locked up after each use, and be

connected to the Internet with a physical cable rather than wirelessly. With the increased security protections afforded by a dedicated computer, transactions executed from those computers could be less at risk.

Officials should also have a written online banking agreement with their financial institution(s) that, at a minimum, complies with GML Section 5-a and a written acceptable use policy (AUP) to inform users about appropriate and safe use of school district computers. The District's acceptable use policy prescribes the development of regulations for computer use.

Officials Did Not Secure Online Banking Transactions

Officials adopted an AUP that details acceptable and unacceptable computer usage and restricts computer usage to purposes that are part of the District's educational mission including, but not limited to, instruction, assessment, administration, research, professional development or other tasks associated for staff assignments. Use of computers for any other purposes is prohibited. The regulations prohibit the wasteful use of these resources.

In addition, while the District developed an adequate online banking policy, its bank agreement was inadequate and the District did not have a separate computer dedicated for online banking transactions. We also found excessive personal web browsing on District computers, which violates the District's AUP.

Bank Agreement – While the District uses one bank to process online transactions that include electronic and external wire transfers and Automated Clearing House (ACH) payments,[1] officials did not have a copy of the banking agreement the District entered with its bank. As a result, the Treasurer had to contact the bank to get a copy of the complete banking agreement.

Our review of the agreement found it was inadequate because it did not:

- Outline how electronic or wire transfers should be accomplished,
- Identify the names and numbers of the bank accounts from which transfers may be made,
- Identify individuals authorized to request the transfer of funds, and
- Detail security procedures to verify payment orders or detect errors in transmission or content of the payment order.

Because officials did not have an adequate banking agreement, they could not ensure that employees were aware of their responsibilities or that funds were adequately secured during online transactions. As a result, users conducting online banking and users of the computers used to conduct online banking

1 The ACH is an electronic network used to process large volumes of electronic payments between banks.

could unintentionally expose online bank accounts to various threats, such as unauthorized access and malicious software, which could potentially lead to a misappropriation of funds without detection.

Authorized Online Banking Access – District officials did not dedicate a separate computer for online banking activities and, as a result, there was an increased risk that unauthorized individuals could potentially gain access to the District's online bank accounts. Instead, the Treasurer and Business Administrator used their District-provided desktop and laptop computers, which they also used to perform their other day-to-day job duties. Although the Superintendent is an authorized online banking user, he was not provided his online banking login credentials and fob from the bank for the two-factor authentication. Furthermore, the Business Administrator had permissions which would allow him to perform all aspects of an online banking transaction, which increases the risk that funds could be misappropriated without detection.

The Treasurer performs all online banking transactions and completes wire transfers and ACH payments, while the Business Administrator reviews the bank statements and approves wire transfers. Due to the various control weaknesses, we reviewed all online bank transfers totaling approximately $37.8 million for the period July 1, 2020 through February 28, 2022 and two months of wire transfers and ACH payments totaling approximately $2.8 million and found they were for appropriate purposes.

Because we identified certain sensitive IT security weaknesses related to accessing the online banking website, we also reviewed the web browsing history on five District computers assigned to the three authorized online banking users. We identified web browsing history for 32 different users' profiles on the Treasurer's desktop which was not reasonable. The Treasurer stated that she allowed other employees to use her computer during new employee onboarding and to assist employees when they had login problems for the District's financial software application. She should not be doing this because allowing other employees to use her computer increases the risk of potential malicious malware infections. In addition, we found incidental personal Internet use by the Treasurer and Superintendent on their District-assigned computers and excessive personal Internet use by the Business Administrator on his District-assigned computers, all of which is prohibited by the District's acceptable use policy.

A portion of the Business Administrator's excessive personal use can be attributed to him synchronizing his web browsing activity between his District and personal devices. However, of the 19,499 personal websites visited (Figure 1), 17,674, or 91 percent, occurred during District business hours.

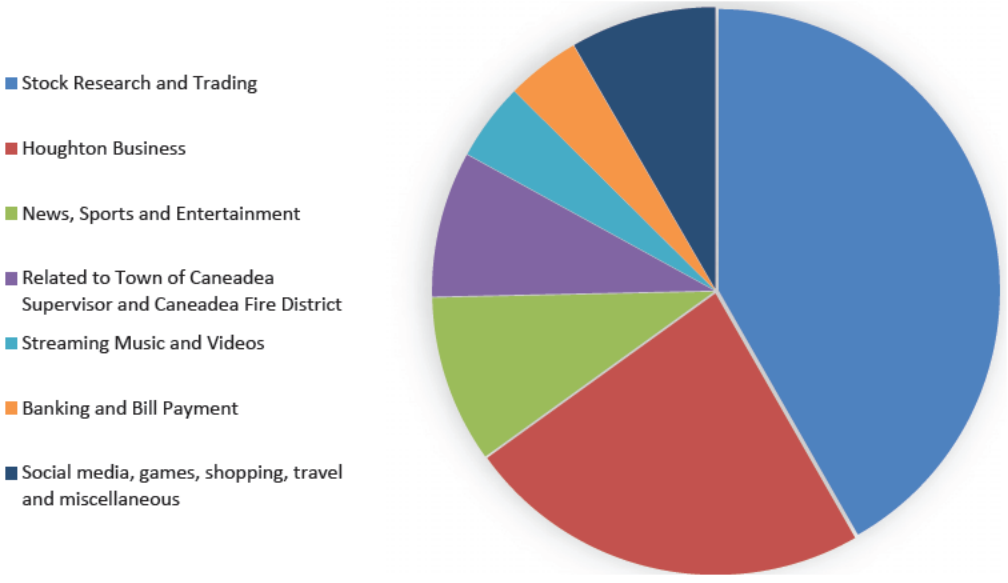
FIGURE 1

Business Administrator's Websites Visited December 13, 2021 - March 11, 2022 With Some Outlier Dates

The Business Administrator's personal web browsing history included websites for stock research and trading, shopping, news and entertainment, online gaming, streaming videos and music, personal banking, personal email, and conducting business as the Town of Caneadea Supervisor and Caneadea Fire District Secretary/ Treasurer, all of which is not allowed by the acceptable use policy (Figure 2).

FIGURE 2

Business Administrator's Personal Website Visits During the Workday



Allowing personal use of computers increases the risk of potential malicious software infections and unauthorized access to the District's online banking website and can decrease employee productivity.

We recognize that District officials took measures to limit potential financial loss by purchasing computer fraud and funds transfer insurance coverage. Although this may provide some financial reimbursement from actual losses, it does not prevent the District's initial financial loss, or disruption to District operations, in the event of an online banking fraud. However, having complete agreements that appropriate officials have access to, monitoring usage and dedicating a computer for online banking would reduce the District's risk of funds being misappropriated and operations disrupted due to a malicious software infection or unauthorized access.

What Do We Recommend?

The Board and Superintendent should:

1. Further investigate the Business Administrator's personal Internet use and take appropriate action as warranted.

The Superintendent and District officials should:

2. Ensure that the written bank agreement is sufficient and that those who perform online banking transactions are familiar with its content.
3. Consider designating one computer to be used for online banking transactions.
4. Review the Business Administrator's permissions and either reduce certain permissions so that he cannot handle all phases of online banking transactions or establish mitigating monitoring procedures.
5. Ensure the Treasurer limits the number of individuals that use her computer.
6. Periodically monitor computer use to ensure compliance with the acceptable use policy and regulations.

Appendix A: Response From District Officials

Mount Morris Central School

30 Bonadonna Avenue, Mount Morris, New York 14510
Phone: 585-658-3331 Fax: 585-658-4814

October 6, 2022

Mr. 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

Unit Name: Mount Morris Central School District
Audit Report Title: Online Banking
Audit Report Number: 2022M-99

Dear Mr. Grant Jr.,

On behalf of the Board of Education and Administration of the Mount Morris Central School District, I would like to thank you and your staff for the guidance provided as a result of this audit. We thank the audit team for its professionalism and communication throughout the process. We have reviewed the draft report issued by your office and we are pleased to confirm that there is no evidence of malfeasance or fraud, and we generally agree with all of your recommendations. In fact, due to the extended timeline for the completion of the audit, the District has had the opportunity to implement several corrective measures ahead of the release of this report.

In June 2022, the District transitioned to the use of a dedicated computer specific to online banking. Also, the District established a Business Office Chromebook that is used to onboard new employees and assist staff members when they are having difficulties connecting to various employee portals. Lastly, the District already had several mitigating monitoring procedures in place prior to the audit related to the Business Administrator's online banking permissions. The Business Administrator does not have the user rights in the District's financial software [redacted] to create a [redacted] file which would be necessary to create an ACH Payroll, and all wire transfers require two District individuals to be involved; the first person to call the wire transfer room at the bank to give the details of the requested transfer and the second person to receive a call from the bank on a recorded line to provide the confirming details of the wire. However, the District is agreeable to the concept of adding any additional mitigating procedures that would strengthen the operation of the District.

See Note 1 Page 8

See Note 2 Page 8

The District disagrees with the key finding that "District officials did not secure access to online banking…[or] ensure that authorized access to online bank accounts was limited." Only two individuals have access to make online banking transactions. The District uses several levels of multi-factor authentication (MFA) to ensure that only these authorized individuals are accessing online banking. Online banking transactions are limited to authorized users who must login using a unique user ID and password and confirm a passcode from a key fob in their possession that generates a new passcode every 30 seconds. We were pleased that your audit showed no indication that our system was compromised by a third party or individual. We welcome your suggested procedures for implementing new security measures as we all know cybersecurity threats are always evolving.

See Note 3 Page 8

We appreciate the opportunity to respond to the findings and recommendations of this report. The District will implement the recommendations of the State Comptroller's Office. A more detailed Corrective Action Plan (CAP) to implement all recommendations will be completed in the 90 days following the release of the final report. We thank you for assisting us in strengthening the operations and procedures of the District.

Sincerely,

Greg Bump
Superintendent of Schools

Appendix B: OSC Comments on the District's Response

Note 1

While the District has a dedicated online banking computer, the Business Administrator does not use it to conduct online banking.

Note 2

The District does not have procedures in place to ensure all online banking transactions are secure.

Note 3

We observed the Treasurer's key fob unsecured and left unattended on multiple occasions.

Appendix C: 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, our audit procedures included the following:

- We interviewed District officials to obtain an understanding of online banking practices and to obtain any related policies and procedures.
- We reviewed policies and procedures for acceptable use of IT and online banking.
- We observed online banking users' access from logon to logoff for the Business Administrator, Treasurer and Superintendent.
- We inquired with District officials about a written agreement with the bank and reviewed the documentation provided by the bank regarding capabilities for electronic transfers.
- On March 11, 2022 and May 3, 2022, we ran a computerized audit script to export the web history files from the five computers assigned to the three users that had authorized access to the District's online banking. We then examined the exported web history data for indications of personal Internet use.
- We reviewed all online transfers during the period July 1, 2020 through February 28, 2022. We also used our professional judgment to select the months of June and December 2021 to review wire transfers and ACH debits because of known wire transfers for debt payments.

Our audit also examined the adequacy of certain sensitive IT 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 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 Repor*t, which you received with the draft audit report. The CAP should be posted on the District's website for public review.

Appendix D: Resources and Services

Regional Office Directory
www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

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

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/files/local-government/publications/pdf/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

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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

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

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller