REPORT OF EXAMINATION | 2017M-98

Morrisville-Eaton Central School District

Online Banking

July 2017

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

Contents

Report Highlights

Morrisville-Eaton Central School District

Audit Objective

Determine whether District officials ensured online banking transactions were appropriate.

Key Findings

- The Board did not adopt an online banking policy defining authorization, process and monitoring of online banking transactions.
- District officials did not properly review online banking transactions or use a designated computer for online banking transactions.
- Not all employees involved in the online banking process have received Internet security awareness training.

Key Recommendations

For online banking:

- Adopt policies and procedures.
- Ensure all transactions are reviewed in a timely manner.
- Designate one computer to be used strictly for transactions.
- Provide Internet security awareness training to involved employees.

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

Background

The Morrisville-Eaton Central School District (District) is located in the Towns of Eaton, Fenner, Lebanon, Lincoln, Nelson, Smithfield and Stockbridge in Madison County.

The District is governed by the Board of Education (Board), which is composed of five elected members. The Board is responsible for the general management and control of District financial and educational affairs.

The Superintendent of Schools, as the District's chief executive officer, is responsible, along with other administrative staff, for the day-to-day management under the Board's direction. The Treasurer and Deputy Treasurer are responsible for online banking transactions.

Quick Facts	
2016-17 Appropriations	**$15.3 million**
Enrollment	**660**
Employees	**140**

Audit Period

July 1, 2015 – December 31, 2016

Online Banking

Online banking provides a way to directly access funds held in the District's bank accounts. Users can review current account balances and account information, including recent transactions and transfer money between accounts or to external accounts. School districts are allowed to disburse or transfer funds in their custody by using an electronic funds transfer (EFT).

An EFT is the electronic transfer of money from one bank account to another either within a single bank or across multiple banks via computer-based systems without the direct intervention of bank staff. This covers a number of different types of payments, such as wire transfers commonly used for bond payments, investments or other large settlements and other electronic type transfers used for small-dollar and recurring transactions, such as federal and State payroll tax payments.

District officials must ensure that staff securely access banking websites to help reduce the risk of unauthorized transfers from both internal and external sources. It is essential that District officials provide authorization of transfers before they are initiated and establish procedures so the District does not become the victim of cyber fraud and experience financial losses that may not be recoverable.

How Should District Officials Reduce the Risk of Inappropriate Online Banking Transactions?

To safeguard District cash assets, policies and procedures are necessary to properly monitor and control online banking transactions. The Board should adopt a comprehensive written online banking policy to provide guidance for staff concerning the online banking activities the District will engage in. The policy should specify the District employees with authority to process transactions and establish an approval process, such as a second authorization or email alert notification, to verify the accuracy and legitimacy of transfer requests on a timely basis.

District officials should segregate the duties of employees granted access to the District's online banking to reduce the opportunity for an employee to make and conceal errors or inappropriate transactions in the normal course of their duties. District officials should also provide for a regular, independent review of bank statements and supporting documentation to detect and address any unauthorized activity.

Good management practices require limiting the number of users authorized to execute online banking activities and the number of computers used. Authorized online banking users should access the District's bank accounts from one computer dedicated for online banking transactions to minimize exposure to malicious software. District computer users should receive Internet security awareness training to ensure they are aware of potential threats, such as

unknowingly downloading unwanted or malicious software or clicking on links that are part of phishing[1] attacks, which can threaten these accounts.

An Online Banking Policy Was Not Adopted and EFTs Were Not Monitored on a Timely Basis

District officials specified that the Treasurer and Deputy Treasurer are authorized to process online banking transactions and developed secondary approval requirements for EFTs based on each user's access.[2] However, the Board did not adopt an online banking policy that defines the type of online banking activities allowed or the procedures for authorizing, processing and monitoring online banking transactions.

District officials adequately segregated the duties for EFTs. For example, the Treasurer transfers money between bank accounts (at the same bank) and is in charge of EFTs for bond payments and employee tax shelter annuities. The Deputy Treasurer makes all other EFTs, such as State payroll tax payments. The Madison-Oneida Board of Cooperative Educational Services (BOCES) performs the District's accounting function, which includes recording all online banking transactions in the accounting system,[3] processing payroll and preparing the bank reconciliations.

While the bank provides email notifications for each EFT, District officials do not review them to verify transfer accuracy and legitimacy. The Deputy Treasurer and District Clerk, who received notification emails, did not review them. Additionally, while the Treasurer was aware she could receive such alerts through an online banking software feature, she did not use this feature to receive notification emails. Reviewing notifications for completed transfers would provide District officials with an added level of security over online transactions.

A senior BOCES account clerk (clerk) reviews the District's EFTs and the supporting documentation each month when she reviews the bank statement and completes the District's bank reconciliations. However, the clerk does not review bank transactions on a regular basis to monitor online transactions as they occur. As a result, inappropriate transactions could go undetected for longer than necessary because about a month elapses between reviews and more than a

---

1 Phishing attacks could 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.

2 The District's bank requires secondary approval for recurring EFTs of $400,000 or more, nonrecurring EFTs of $500,000 or more and limits EFTs to $1.005 million. The Treasurer and Deputy Treasurer cannot create new EFT recipients without a second approval in the online banking software.

3 The Treasurer and Deputy Treasurer do not have access to the accounting system.

month of online activity has occurred by the time the clerk completes the monthly review.

When District bank accounts are not monitored timely, (at least every two to three days) unauthorized or suspicious activity could occur and not immediately be detected and reported.

A Dedicated Computer Was Not Used for All Online Banking and Security Awareness Training Was Not Provided to All Employees

While the Treasurer uses a computer designated strictly for online banking transactions, the Deputy Treasurer does not. The Deputy Treasurer has not received Internet security awareness training. This lack of training, combined with not always using a dedicated computer for online banking, could result in unintentionally exposing the District's bank accounts to threats from malicious software, which could endanger its assets.

We reviewed two months of online banking transactions. All 79 transactions totaling more than $5.7 million (including 19 EFTs totaling $2.5 million) were for appropriate District purposes.[4]

What Do We Recommend?

The Board should:

1. Establish a written online banking policy that specifies the online banking activities that will be used, the employees authorized to initiate, approve, transmit, review and reconcile EFT transactions and where online banking will be performed (e.g., a dedicated computer).

District officials should:

2. Review online banking transactions regularly and ensure notifications and other security measures available from the District's bank, including email notifications, are used to monitor all EFTs in a timely manner.
3. Designate a computer to be strictly dedicated for online banking transactions.
4. Ensure that employees involved in the online banking process are provided with adequate Internet security awareness training.

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

Appendix A: Response From District Officials

MORRISVILLE-EATON CENTRAL SCHOOL DISTRICT
Post Office Box 990 • Morrisville New York • 13408-0990 • 315-684-9300

Gregory Molloy
Superintendent

Debra Everson
Assistant Superintendent for Finance & Support Services

Debra Dushko
Elementary School Principal

Benjamin New
Middle/High School Principal

Jodi Shantal
District Clerk

July 13, 2017

Syracuse Regional Office
State Office Building Room 409
222 E. Washington Street
Syracuse, NY 13202-1428

Dear Rebecca Wilcox,

Morrisville-Eaton CSD acknowledges the receipt of the comptrollers audit findings and are in agreement of what was reported.

Sincerely,

Gregory Molloy
Superintendent

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 the District's online banking practices.
- We reviewed District policies to determine if the Board has adopted adequate online banking policies.
- We observed online banking user access from log in to log off.
- We made inquiries to District officials about written agreements with banks and online banking and EFT procedures. We reviewed documentation available from the bank regarding capabilities for EFTs.
- We examined the two District computers used to access online banking.
- We reviewed all online banking transactions for two randomly selected months to determine whether they were appropriate District expenditures. We selected November 2015 and June 2016. For these months, we reviewed 60 transfers between bank accounts (at the same bank) and 19 EFTs.

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

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 2116-1(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 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. We encourage the Board to make the CAP available for public review in the Clerk's office.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/localgov/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/localgov/costsavings/index.htm

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/localgov/fiscalmonitoring/index.htm

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/localgov/planbudget/index.htm

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/localgov/lgli/pdf/cybersecurityguide.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/localgov/finreporting/index.htm

Research Reports / Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/localgov/researchpubs/index.htm

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/localgov/academy/index.htm

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.state.ny.us

www.osc.state.ny.us/localgov

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, NY 13202-1428

Tel: (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

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