

Skaneateles Central School District

Online Banking

MARCH 2019



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

Contents

- Report Highlights 1**

- Online Banking 2**
 - How Can Officials Reduce the Risk of Inappropriate Online Banking Transactions? 2

 - Duties are Adequately Segregated but the District’s Policy Does Not Clearly Describe Online Banking Procedures 3

 - Officials Have Established Security Procedures 4

 - A Dedicated Computer Was Used for Online Banking but Security Awareness Training Was Not Provided to Employees 5

 - What Do We Recommend? 5

- Appendix A – Response From District Officials 6**

- Appendix B – Audit Methodology and Standards 8**

- Appendix C – Resources and Services 9**

Report Highlights

Skaneateles Central School District

Audit Objective

Determine whether District officials ensured online banking transactions were appropriate and secure.

Key Findings

- Officials adequately segregated the duties of employees responsible for online banking transactions and adequately established security procedures over online banking. All online payments and transfers totaling \$72 million during our audit period were appropriate.
- The online banking policy does not clearly indicate how online transfers will be authorized and processed.
- 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 employees involved in online banking receive Internet security awareness training.

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

Background

The Skaneateles Central School District (District) serves the Towns of Niles, Owasco and Sennett in Cayuga County and the Towns of Marcellus, Skaneateles and Spafford in Onondaga County.

The District is governed by a Board of Education (Board), which is 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 Assistant Superintendent for Business Operations (Business Administrator) is responsible for overseeing these transactions.

Quick Facts

Employees	420
Enrollment	1,360
2018-19 Appropriations	\$34 million
Online Banking Transactions During Audit Period	575
Dollar Amount of Online Banking Transactions During Audit Period	\$72 million

Audit Period

July 1, 2017 – August 31, 2018

Online Banking

Online banking provides a way to directly access funds in district bank accounts. Users can review current account balances and account information, including recent transactions and transfer money between 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. It is essential that district officials provide authorization for transfers before they are initiated and establish procedures to ensure that staff are securely accessing banking websites to reduce the risk of unauthorized transfers from internal and external sources.

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

A board should adopt policies and procedures to monitor and control online banking transactions. A comprehensive written online banking policy clearly describes the online activities district officials may engage in, specifies which employees are authorized to process transactions, establishes a detailed approval process to verify the accuracy and legitimacy of transfer requests and provides for the review and reconciliation of transfers.

Procedures should ensure transactions are appropriate and secure. Officials should segregate the duties of employees granted access to 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 provide for a regular, independent review of bank statements and supporting documentation to detect and address any unauthorized activity. Employees should have unique usernames and passwords that should not be 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.

A district should have an agreement with its bank that prescribes the manner in which transfers will be accomplished, identifies the names and numbers of the bank accounts from which such transfers may be made and identifies the individuals authorized to request transfers. The agreement should implement security procedures that include verifying that payment orders are that of the district and detecting errors in the transmission or content of such payment orders.

Good management practices should not only limit the number of users authorized to execute online banking activities, but also limit the computers for such activities. Authorized users should only access bank accounts from a dedicated

¹ General Municipal Law Section 5-A

computer. Other computers may not have the same security protections, and transactions executed from those computers could be more at risk. Employees with online banking access should receive Internet security awareness training to educate them on safe computing practices, such as avoiding untrusted websites and unknowingly downloading unwanted or malicious software.

Duties are Adequately Segregated but the District’s Policy Does Not Clearly Describe Online Banking Procedures

The Board adopted an online banking policy that designates employees who can process online transactions, requires segregation of duties and requires each user to have a separate user name and password. It also requires at least two individuals be involved in each transaction and someone independent of the online banking process to review a monthly report of all online banking activity and reconcile it with bank statements. Lastly, it requires, whenever possible, the recording function to be delegated to a third individual.

District officials have adequately segregated the duties for online banking. The Treasurer, Deputy Treasurer and Business Administrator can initiate and approve intrabank transfers between District bank accounts and make payments to third parties via Automated Clearing House (ACH) and wire transfer. The Treasurer typically initiates the transfers and payments and the Deputy Treasurer typically approves the transactions. The Business Administrator typically does not perform any online banking transactions; however, she has access as a backup in case the Treasurer or Deputy Treasurer are unavailable to initiate or approve a transaction. Although the Business Administrator and Treasurer have the ability to record transactions, the District’s required dual approval of transactions and pre-authorization of bank accounts to make wire transfers to and from, helps to mitigate the risk of improper transfers occurring and being concealed. The Business Administrator reviews bank reconciliations and supporting information compiled by the Treasurer. The bank statements show all online banking transactions, and the Treasurer prints a monthly report showing all activity for each bank account (which includes all online banking transfers). Lastly, users are required to enter a unique username and password to log into the online banking platforms and the credentials are not shared. Also, advanced authentication techniques are employed by the online banking platforms. Individual passwords and advanced authentication help to ensure only authorized and secure access is granted to the online banking platforms.

Although officials have established procedures, the adopted policy does not clearly convey the specific procedures to be used or how online transfers will be approved. Also, it contains outdated information. For example, the policy states, “Online transactions must be authorized by the District’s Business Official,” yet it does not specify how authorization will be granted or documented.

Furthermore, the policy 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 or an internal audit function. In July 2018, the Board adopted a resolution authorizing District administration to refine and update the District’s policy manual. The Business Administrator stated that the online banking policy, as a component of the policy manual, was to be updated.

Officials Have Established Security Procedures

District officials maintain accounts, with online transfer capabilities, at a bank, and within an intermunicipal investment cooperative fund (investment fund).² Account terms, conditions and settings, established by both the bank and investment fund, and agreed to by District officials, prescribe the manner in which electronic and wire transfers will be accomplished, identify the names and numbers of the accounts from which such transfers may be made and identify the individuals authorized to request transfers. Security procedures have been implemented, for accounts at the bank and investment fund to prevent and detect unauthorized external transfers.

Bank Accounts — A single user can add a new account as an external transfer option. However, two users are required to execute an electronic or wire transfer to the new account – one user to initiate the transfer and a different user to approve and complete the transfer. Both the user who initiated and the user who approved the transfer receive an email that a transfer occurred.

Investment Fund Accounts — A new account may only be added as an external transfer option after two authorized users complete and sign a paper request form authorizing the new account. Currently, the only accounts approved for external transfers are District accounts at other financial institutions. Once an external account has been approved for transfers, a single user can both initiate and complete an electronic or wire transfer to that account. However, when an external transfer is made, emails are sent to all authorized District users that a transfer occurred.

We reviewed all 575 online banking transactions totaling \$72 million during our audit period. A majority (561 totaling \$55.8 million) were transfers between District accounts at the same bank, and we ensured that all outgoing debits equaled incoming credits. We viewed supporting documentation for the remaining 14 external transfers totaling \$16.2 million and confirmed they were for appropriate purposes.

² Articles 5-G and 3-A of GML provide the authority for school districts and most local governments to enter into intermunicipal cooperation agreements to invest idle funds on a cooperative basis with other school districts and local governments, subject to certain requirements.

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

The District has one computer that is used exclusively to access the District's online accounts. This computer has wired access to the Internet and is not connected to a network, which are added security protections that can safeguard financial transactions.

However, Internet security awareness training was not provided to the three employees with access to make electronic payments or wire transfers. The lack of training increases the risk that users could unintentionally expose online bank accounts to threats from malicious software, which could endanger cash assets.

We reviewed the website browsing history on the dedicated computer to determine if employees had visited websites other than those necessary to conduct online banking. We did not identify any non-banking websites that were visited by employees.

What Do We Recommend?

1. The Board should update the online banking policy to ensure it clearly describes the procedures for authorizing and processing online banking transactions.
2. District officials should ensure that employees involved in the online banking process receive Internet security awareness training.

Appendix A: Response From District Officials



Skaneateles Central School District

*Nationally Recognized for Excellence
45 East Elizabeth Street
Skaneateles, New York 13152*

Lynda Quick
Superintendent of Schools
(315) 291-2221

Christine DeMass
Assistant Superintendent for Business Operations
(315) 291-2268
Fax (315) 685-0347

March 19, 2019

Rebecca Wilcox, Chief Examiner
NYS Comptroller
Division of Local Government and School Accountability
Syracuse Regional Office
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428

Re: Skaneateles Central School District
Online Banking
Report of Examination 2019M-2

Dear Ms. Wilcox:

This is a response to the audit report conducted by the Office of the New York State Comptroller for the Skaneateles Central School District. The period covered by the examination report is July 1, 2017 – August 31, 2018. This letter will also serve as the District's Corrective Action Plan.

On behalf of the Board of Education and community, we would like to thank the staff at the New York State Comptroller's Office for taking the time to review, analyze and suggest ways to improve our Online Banking procedures in the district. We are constantly looking at ways to develop our practices, and look at this report as a tool to help us target areas where we can improve. The district is in general agreement with the findings included in the Draft Report.

The central office administrators and staff have already started to address the key findings outlined in the audit results.

Online Banking Policy

Audit Recommendation: The Board should update the online banking policy to ensure it clearly describes the procedures for authorizing and processing online banking transactions.

The District agrees that the Online Banking policy in place at the time of the audit could be updated to align with our practices. At the January 22, 2019 regular meeting, the Board of Education adopted revised policy 5510 Accounting of Funds, which addresses online banking. The policy was updated to include that the District Business Official must authorize access and permissions for all online users. The revision also removed the statement "The Internal Auditor will periodically confirm that the wire transfers have appropriate signatures, verification and authorization of proper personnel".

Skaneateles High School
Gregory Santoro
(315) 291-2231

Skaneateles Middle School
Michael Caraccio
(315) 291-2241

State Street Intermediate School
Michelle Crisafulli
(315) 291-2261

Belle H. Waterman Primary School
Patrick J. Brown
(315) 291-2351

The District does not have an internal auditor and is not required to have one due to Subdivision 2 of section 2116-b of Education Law. The law states that districts with an actual enrollment of less than 1,500 students in the previous school year are exempt from the requirement to establish or maintain an internal audit function. In addition, clarifying language was added to define that the District Treasurer will reconcile monthly bank statements with the District's accounting software reports. This practice was already being completed but was not specifically outlined in the policy.

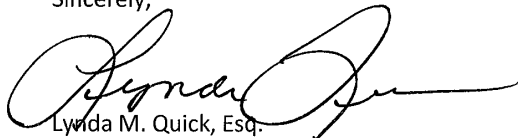
Internet Security Awareness Training

Audit Recommendation: District officials should ensure that employees involved in the online banking process receive Internet security awareness training.

Our staff is aware of the security features that are in place by our banking institution. However, we agree that overall Internet security awareness training could benefit the District. In December 2018 and January 2019, all staff with access to online banking received training suggested by the New York State Comptroller's office. This training included cyber security training videos that can be found on the Office of Information Technology Services website. Administration will further review the resource, Protecting Sensitive Data and Other Local Government Assets: A Non-Technical Cybersecurity Guide for Local Leaders, and develop an ongoing training plan.

Please feel free to reach out to me with any questions. Thank you.

Sincerely,



Lynda M. Quick, Esq.
Superintendent of Schools

Skaneateles High School
Gregory Santoro
(315) 291-2231

Skaneateles Middle School
Michael Caraccio
(315) 291-2241

State Street Intermediate School
Michelle Crisafulli
(315) 291-2261

Belle H. Waterman Primary School
Patrick J. Brown
(315) 291-2351

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, our audit procedures included the following:

- 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 if the Board adopted an adequate online banking policy.
- We inquired about 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 computer used to access online banking and reviewed its website browsing history.
- We identified and examined all online banking transactions during our audit period. For intrabank transfers we ensured daily amounts debited from District accounts equaled amounts credited to District accounts. For external transfers we reviewed supporting documentation to ensure the transfers were appropriate.

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.

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 District 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/pubs/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/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.ny.gov

www.osc.state.ny.us/localgov/index.htm

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)