REPORT OF EXAMINATION | 2021M-164

South Seneca Central School District

Online Banking

JUNE 2022

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

Contents

Report Highlights

South Seneca Central School District

Audit Objective

Determine whether the South Seneca Central School District's (District) Board of Education (Board) and District officials ensure online banking transactions are appropriate and secure.

Key Findings

The Board and District officials did not ensure that online banking transactions were appropriate and secure.

- District officials improperly allowed a third-party administrator to access a District bank account.
- The Board's online banking policy (Policy) dated April 24, 2013 has not been updated or reviewed. It does not reflect current online banking practices and it assigns oversight responsibilities to an internal auditor. However, the District does not have an internal auditor and these responsibilities were not assigned to another employee.
- Bank agreements do not contain sufficient authorization controls.
- A dedicated computer was not used to conduct online banking and none of the employees involved in online banking received Internet security awareness training.

Key Recommendations

- Discontinue allowing third-party administrator access to a District bank account.
- Update the Policy and perform online banking transactions on a dedicated computer.
- Amend the bank agreements to require another District official to approve electronic transfers.

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

Background

The District serves the Towns of Covert, Lodi, Ovid and Romulus in Seneca County and the Town of Hector in Schuyler County.

The District is governed by an elected seven-member Board responsible for the general management and control of financial and educational affairs. The Superintendent serves as the chief executive officer responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The Business Administrator, Treasurer and Deputy Treasurer are responsible for overseeing and performing online-banking activity. The Treasurer is responsible for the custody and disbursement of all funds.

Quick Facts	
2020-21 Appropriations	$25 million
Online Banking Activity for the Audit Period	
Transactions	1,089
Dollar Amount	$70 million

Audit Period

July 1, 2019 – January 31, 2021. We extended our scope back to July 1997 to review certain bank agreements and forward to April 2021 to review website browsing history.

Online Banking

Online banking provides a way to directly access funds in a school district's bank accounts. Users can review current account balances and information, including recent transactions, and transfer money between district accounts or to external accounts.

A school district's treasurer is generally responsible for the disbursement of all money, including electronic payments.

How Should a Board and Officials Safeguard Online Banking Transactions?

A school district's treasurer is generally responsible for the disbursement of all money, including electronic payments. Districts that self-fund healthcare benefits are permitted to enter into an agreement with a qualified third-party administrator to audit, approve and pay benefit claims on the district's behalf. Districts that self-fund healthcare benefits are permitted to transfer money to a third-party administrator in the total amount of benefit claims audited and approved by the third-party administrator for disbursement by the third-party administrator. However, districts are not authorized to provide a third-party administrator with access to withdraw funds from district bank accounts. Any electronic disbursement of money should be completed and controlled by the treasurer.

A 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.

School districts can disburse or transfer funds by electronic funds transfers (EFTs), provided that the governing board enters into a written agreement with the bank. A school district's banking agreements must prescribe the manner in which transfers can be made and identify the individuals authorized and the bank accounts that can be used for online transfers. The agreement must 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.

Bank accounts should be monitored frequently, at least every two or three days. In addition, regular, independent reviews of bank statements and supporting documentation should be performed to help detect any unauthorized or suspicious activity.

Officials also should limit the number 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 which are relevant and specific to their job duties and responsibilities.

A Third-Party Administrator Had Access to District Funds

The Treasurer provided the third-party administrator direct access to a District bank account to process dental claims. The Treasurer told us she monitored the Automated Clearing House (ACH) transactions performed by the third-party administrator by reviewing dental claim invoices. ACH are transactions in which funds are moved from one bank to another bank. However, there is no legal authority for the District to allow third parties to access and disburse funds from District bank accounts. During the audit period, the third-party administrator made 81 withdrawals totaling almost $125,000 from a District bank account. The Treasurer told us she was unaware that this was impermissible. When the District allows outside parties to access and disburse funds from its bank account, there is an increased risk that unauthorized or inappropriate disbursements could be made.

Controls Over Online Banking Transactions Should Be Improved

We reviewed 85 online banking transactions totaling $6.6 million that were processed during the audit period and found they were all for appropriate purposes. While we found online banking responsibilities for initiating and approving online transactions were segregated, the Board should update the Policy and improve the District's approval and/or notification processes for all transactions and monitoring and security procedures for online banking.

Online Banking Policy – The Policy was last revised by the Board on April 24, 2013 and has not been reviewed or updated to include the District's current online banking procedures. The Policy identifies who can conduct online banking transactions and requires staff independent of the online banking process to reconcile monthly reports of all online banking activities to the bank statements. It does not specifically identify what transactions employees authorized to conduct online banking can perform or how online transactions should be approved.

Although the Policy states the Business Administrator must authorize all online transactions, it does not specify how approval should be granted or documented. The Policy also states: "The Internal Auditor will periodically confirm that wire transfers have appropriate signatures, verification and authorization of proper personnel during annual risk assessment." The District does not have an internal auditor or an internal audit function to perform this review and this responsibility was not assigned to someone else.

The Policy was last revised on April 24, 2013 and has not been reviewed or updated to include the District's current online banking procedures.

Online Banking Agreements and Transaction Authorizations – EFTs are transactions in which funds are transferred to a third party. Officials execute EFTs at one bank, with appropriate pre-approvals, by requiring another District official to electronically approve the transaction before the bank will execute it. We reviewed five external transfers totaling almost $2.9 million and found they were properly authorized and for appropriate District purposes.

The District processes ACH payments at three of its banks. Two of three banks execute ACH transactions without further involvement or approval of any other District official. The two banks send an email with transaction details to the Treasurer who processed the transaction. The third bank requires two officials, an initiator and another official to pre-approve, before it will execute the transaction. We reviewed 55 ACH transfers totaling almost $550,000 and found they had approved authorization letters and that they were for appropriate District purposes.

Internal transactions are transactions in which funds are transferred to one or more other District bank accounts. The District processes internal transactions at three banks and one local government investment cooperative (cooperative). The cooperative sends confirmation emails to the Treasurer and Business Administrator, while the three banks do not. We reviewed 25 internal transfers totaling about $3.1 million and found they had approved authorization letters and that they were for appropriate District purposes.

The Treasurer told us she provides the Business Administrator a written description of the transactions for signoff prior to processing them for all three banks and the cooperative. However, only one bank requires pre-approval to execute a transaction by the Business Administrator pursuant to the online banking agreement in place with that bank. The other two banks and the cooperative do not have a pre-approval process in place as it is not included in their online banking agreement with the District. Without bank notification to another District official or electronic approvals to execute transactions, there is an increased risk that inappropriate transactions and errors could be made and not identified.

Without bank notification to another District official or electronic approvals to execute transactions, there is an increased risk that inappropriate transactions and errors could be made and not identified.

Monitoring of Online Banking Transactions – Although required by the Policy, the District does not prepare a monthly report of all online banking activity. As a result, staff independent of the online banking process cannot review such a report and reconcile online banking transactions to the bank statement which would help identify any unauthorized or suspicious activity. The Business Administrator told us that the limited staffing in the District Business Office prevented the preparation of the monthly report and its review and reconciliation.

The Business Administrator told us he reviews the bank reconciliations and reconciling items, prepared by the Treasurer, for reasonableness. However, the

Business Administrator does not receive supporting documentation for online banking transactions. While one bank provides a pre-approval confirmation to the Business Administrator before the bank will execute the transaction, none of the banks provide the Business Administrator any confirmation of executed transactions. Absent any ability to oversee online transactions, District officials have less assurance that all transactions are appropriate.

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 and that she was unaware of the need for consistent and timely reviews. Without timely reviews, inappropriate transactions may not be identified in time for any stolen money to be recovered.

Also, the Policy states the Internal Auditor will periodically confirm that wire transfers have appropriate signatures, verification and authorization of proper personnel during the annual risk assessment. However, the District does not have an internal auditor to perform this assessment and this responsibility was not assigned to someone else.

Computer Access Restrictions – We reviewed the three banks that conduct external banking transactions. All three banks used by the District to conduct online banking have the capability to restrict account access to only computers specified by the District. Two banks did not restrict access to specific computers and, although restrictions have been enabled at one bank, their list of computers granted access included one that it is no longer used and approved to conduct online banking.

The Business Administrator told us that specific computer restrictions were not enabled because he wanted to retain the ability to execute online transactions using other computers at remote locations without the additional process of adding new authorized computers. Enabling restrictions to computers specified by the District would help limit the computers that could be used to access the District's online bank accounts, and thus help minimize the opportunities for malicious users to gain unauthorized access and process unapproved transactions.

Without a thorough review of the monthly bank reconciliations, a timely review of all online banking transactions, and a critical review of transactions by someone independent of the process, there is an increased risk that unauthorized online banking transactions are executed.

Dedicated Computer – The Policy states that online banking will only take place on secure District computers located inside the Treasurer's or Business Office but does not require a dedicated computer be assigned for online banking. The Business Administrator and Treasurer used their assigned District computers to conduct online banking and also for non-banking purposes. We reviewed the

website browsing history on the computers used by the Business Administrator and Treasurer and found they were used to conduct online banking and also for email and browsing various websites including those unrelated to their job duties and responsibilities such as personal banking and social media, sports pages and vacation sites. Email and Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality, integrity or availability while making funds vulnerable to online theft through unauthorized access. Therefore, online banking should be conducted on a dedicated computer as this practice can help minimize a system compromise.

Internet Security Awareness Training – We also found that Internet security awareness training was not provided to the Business Administrator or Treasurer. The Network Administrator told us only staff that fail a periodic phishing test are required to complete online Internet security awareness training. There is no training offered to all staff other than those that fail the phishing test. The Business Administrator was not sent a phishing test and the Treasurer did not fail the phishing tests; therefore, they did not receive training. Nonetheless, to ensure individuals who use the District's computers are aware of cyber threats and how to identify them, security awareness training should be periodically provided to all staff.

… Internet security awareness training was not provided to the Business Administrator or Treasurer.

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.

What Do We Recommend?

The Board should:

1. Update the Policy to clearly describe the procedures for processing, authorizing and reviewing online banking transactions, such as specifying how approvals should be granted and documented. In addition, it should identify the title of person employed at the District who should periodically confirm wire transfers for appropriateness and proper approvals.

2. Amend the bank agreements to require pre-approvals for electronic transfers and provide written confirmations to other District officials for all online banking activity once the requested funds have been transmitted.

District officials should:

3. Ensure that the reconciliation of transfers includes the review of supporting information for each electronic transaction.

4. Review online banking activity on a timely basis (every two to three days) to detect any unauthorized activity.
5. Ensure that the Treasurer cannot execute external online banking transactions without approval.
6. Discontinue allowing third parties from having access to the District's bank account.
7. Periodically review the restrictions on the computers that are allowed access to online banking to ensure they are appropriate.
8. Ensure that a dedicated computer is used to perform online banking transactions.
9. Ensure that employees who are involved in the online banking process receive Internet security awareness training, at least annually, to stay up-to-date with current threats and social-engineering techniques.

Appendix A: Response From District Officials

SOUTH SENECA
CENTRAL SCHOOL DISTRICT

Telephone Number: 607-869-9636 /// 7263 South Main Street, Ovid, NY 14521 /// **Fax Number:** 607-869-2529

Stephen J. Parker Zielinski /// *Superintendent of Schools* /// szielinski@southseneca.org

April 25, 2022

Julie Landcastle, Chief Examiner
Office of the State Comptroller
Division of Local Government and School Accountability
State Office Building, Suite 1702
44 Hawley Street
Binghamton, NY 13901-4417

Dear Ms. Landcastle,

The South Seneca Central School District is in receipt of your findings related to the recently completed audit of our Online Banking practice. We thank the audit team for its professionalism and communication throughout the process, and we agree with all findings.

Because the timeline for completion of the audit was an extended one, we have had the opportunity to substantially address each of the key recommendations ahead of the audit's publication. Each of the district's new policies and procedures will be included in our corrective action plan, as required.

Specifically, in response to feedback from the audit team during the process, South Seneca has transitioned to the use of a dedicated computer specific to online banking; has discontinued the use of third-party access to accounts; has implemented new approval protocols internally for electronic transfers; and is amending our board policy to reflect current practice.

We appreciate the opportunity to have our questions answered throughout, and know that the security of our banking has been improved as a result of the process.

Sincerely,

Stephen J Parker Zielinski, 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, our audit procedures included the following:

- We interviewed District and banking officials to obtain an understanding of online banking practices and District officials to 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 three banks and one cooperative and reviewed documentation regarding capabilities for electronic transfers.
- We observed online banking user access from logon to logoff for the Treasurer and Business Administrator.
- We examined the computers used to access online banking, exported the website browsing history in April 2021 using a computerized exporter script and reviewed their website browsing history.
- We identified 1,089 online banking transactions totaling $70,406,591 during our audit period and examined 85 transactions totaling $6,602,451. The 85 transactions consisted of all 25 internal transfers totaling $3,158,415, five external wire transfers totaling $2,899,656 and 55 ACH payments totaling $544,380.
- We verified that all internal 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 reviewed the District's phishing simulation results to determine if those involved in online banking passed or failed the District's phishing efforts.

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/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

STATEWIDE REGIONAL OFFICE – Julie Landcastle, Chief Examiner

Utica State Office Building, Room 604 • 207 Genesee Street • Utica, New York 13501

Tel (315) 793-2484

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