New York State Comptroller
THOMAS P. DiNAPOLI

Huntington Union Free School District

Online Banking

2022M-178 | January 2023

Division of Local Government and School Accountability

Contents

Report Highlights

Huntington Union Free School District

Audit Objective

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

Key Findings

While we determined that online banking transactions were appropriate, the Board and District officials did not meet all the requirements of General Municipal Law Section 5-A and must improve controls over online banking to ensure these transactions are secure.

- District officials did not enter into adequate written agreements with the District's banking institutions, and the Board did not adopt an online banking policy.
- District officials did not adequately segregate online banking duties or require secondary authorization for online payments and transfers.
- Employees who performed online banking activities did not receive Internet security awareness training during our audit period.

Key Recommendations

- Adopt an online banking policy and enter into adequate written agreements with banking institutions.
- Adequately segregate online banking duties.
- Provide periodic Internet security and awareness training to employees who perform online banking activities.

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

Background

The Huntington Union Free School District (District) serves the Town of Huntington in Suffolk County. The District is governed by a seven-member Board of Education (Board).

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 is responsible for performing online banking transactions, and the Assistant Superintendent for Finance and Management (Assistant Superintendent) is responsible for overseeing these transactions.

Quick Facts

Total Online Banking Transactions During Audit Period	$299.8 million
Electronic Transfers Reviewed	$153.9 million
Electronic Payments Reviewed	$22.9 million

Audit Period

July 1, 2020 – May 31, 2022

Online Banking

Online banking provides a way to directly access funds held in a school district's (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. Because large sums of money can be transferred easily and quickly between accounts, district officials must establish adequate controls to ensure online banking transactions are appropriate and secure.

How Should a Board and District Officials Safeguard Online Banking Transactions?

A board and district officials should comply with New York State General Municipal Law Section 5-A (GML) that allows districts to disburse or transfer funds by electronic funds transfers (EFTs), provided that the governing board enters into a written agreement with the district's bank. An EFT is the electronic transfer of money from one bank account to another, either within a single bank or across multiple banks, through computer-based systems without the direct intervention of bank staff. A bank agreement must describe the manner in which EFTs will be accomplished and identify the names and numbers of bank accounts from which transfers may be made and the individuals authorized to request transfers.

The board and district officials must also implement a security procedure that includes verifying that payment orders are for the initiating district and reviewing payment orders to detect errors in transmission or content.

In addition, a board should adopt a comprehensive written online banking policy and periodically review and update it. This policy should at a minimum:

- Clearly describe the online activities that district officials may perform.
- Specify which employees are authorized to initiate, approve, transmit and record these transactions.
- Establish an approval process to verify the accuracy and legitimacy of transfer requests.
- Require authorized staff to review and reconcile transfers.

At least two individuals should be involved in each electronic transaction. Authorizing and transmitting duties should be segregated. If possible, recording duties should be performed by someone who does not have authorizing or transmitting duties. Officials also should frequently monitor district bank accounts to help detect unauthorized or suspicious activity.

Where possible, users should access bank accounts only from a dedicated computer. Other computers used for everyday purposes may not have the same security protections as a computer dedicated to online banking. Consequently,

using other computers to perform online banking could create more risk. For example, accessing email and browsing the Internet increases the likelihood that a computer will be exposed to threats that may make District funds vulnerable to theft through unauthorized access.

In addition, staff members who access online banking functions should receive Internet security awareness training to educate them on safe computing practices. These practices include avoiding untrusted websites, not clicking on links from untrusted sources and not opening suspicious email that appears to be from trusted sources.

Officials Should Improve Controls Over Online Banking Transactions

The District maintains accounts with online transfer capabilities at two banks. At one bank, the Treasurer performs EFTs between its eight accounts at the bank and to accounts at other financial institutions. The District has four district accounts and nine extra-classroom activity accounts (ECAs) at another bank.

At the second bank, the accounts payable clerk can transfer funds between its 13 accounts. While we determined that online banking transactions were appropriate, the Board and District officials should improve controls over online banking to ensure these transactions are secure.

Online Banking Policy and Written Agreements – The District did not retain copies of its bank agreements. Upon our request, the Treasurer obtained copies of the written agreements with each bank.

The agreement with the first bank consisted of terms of service for access, but did not require District officials to sign the agreement acknowledging these terms. In addition, the agreement did not meet all the requirements of GML.[1] It did not identify, by number or name, the accounts from which EFTs may be made. Also, the agreement did not identify which District officer or officers were authorized to order EFTs.

Although the agreement identified security procedures, including the use of an approved security device to access the accounts online, the agreement does not address procedures to verify payment orders or detect errors in transmission or content of the payment order. Instead, the agreement stated that the District would appoint security administrators who would be responsible for managing online account settings and establishing user accounts, access and permissions.

The Treasurer and Assistant Superintendent were the security administrators on the accounts and were the only two individuals who could access the accounts online. The Treasurer had full access to perform all online transactions, and

1 Section 5-A

the Assistant Superintendent was limited to approving templates for repeat transactions. However, as security administrators, the Treasurer and Assistant Superintendent could change their access levels.

The Treasurer signed and dated the agreement with the second bank in April 2005. However, the agreement did not identify, by number or name, the accounts from which EFTs could be made as required by GML.[2] Also, the agreement did not identify which District officer or officers were authorized to order EFTs.

A bank representative told us that the District could transfer between all accounts within the bank, but could not make payments or transfers to outside banks. Access to online banking for the second bank was limited to one user: an accounts payable clerk (clerk) in the business office. The Treasurer and two central treasurers for ECAs were the signatories on these accounts. However, the clerk was not a signatory.

The clerk had this access to perform transfers between ECA accounts. However, she also could access all District accounts at the second bank. During our review of online activity, we did not find any transfers between the ECA accounts and other District accounts at this bank.

The Board did not adopt an online banking policy to describe the online activities that District officials were authorized to perform, specify which employees were authorized to process transactions, establish an approval process to verify the accuracy and legitimacy of transfer requests, or require authorized staff to review and reconcile transfers.

Without an online banking policy, District officials cannot ensure that employees are aware of their responsibilities. Without an adequate online banking agreement, including a pre-approval process and security procedures to verify that payment orders are legitimate, the District has an increased risk that inappropriate transactions and errors could occur and remain undetected.

Segregation of Duties – District officials did not adequately segregate online banking duties. For example, the Treasurer and clerk could make intrabank transfers without obtaining authorizations. In addition, the Treasurer could initiate and approve payments to third parties through automated clearing house (ACH) and wire transfers.

The Treasurer and Assistant Superintendent were security administrators for online banking at the first bank and had their own username, password and security token for accessing the online banking platform. However, they were the only online banking users, and each had the ability to modify their access rights.

2 Ibid.

The Treasurer initiated and approved intrabank transfers and electronic payments, including payments from templates, wire payments and electronic checks. The Assistant Superintendent and Treasurer told us that electronic payments could be made only through templates that were approved by the Assistant Superintendent. However, the Assistant Superintendent did not approve individual transactions.

Also, the Treasurer could create, delete, modify and approve templates, payments and transfers. However, these transactions did not require secondary authorization and approval. The Treasurer and Assistant Superintendent received automated email alerts when electronic payments were scheduled, but not for intrabank transfers.

The Assistant Superintendent, Treasurer and clerk told us that the clerk made intrabank transfers only for ECA accounts at the second bank. Because the clerk was the only user on the account at the second bank, she had access to all District accounts at this bank.

We reviewed six months of online transactions,[3] which included 98 electronic payments totaling $22.9 million and 103 intrabank transfers totaling $153.9 million, and determined that they were for appropriate District purposes. However, without proper segregation of duties and controls over online banking access, the District has an increased risk that inappropriate transactions or errors could occur and remain undetected.

Dedicated Computer and Cybersecurity Training – District officials did not use a dedicated computer to process online banking transactions. Instead, the Assistant Superintendent, Treasurer and clerk accessed online banking software applications from their assigned District computers. However, they used these computers for all other work-related activities, including connecting to the Internet.

We examined the web browsing history for each computer and determined that these individuals used the computers to conduct their assigned District duties and for other incidental uses. To the extent possible, authorized users should access online bank accounts from one computer dedicated for online banking to minimize exposure to malicious software.

While Internet security and awareness training was given to administrators and educational staff, the Treasurer, clerk and other business office staff were not given this training. After we discussed this finding with officials, the District provided Internet security and awareness training to the business office staff before the end of our fieldwork. Topics from the training included sessions on phishing campaigns, ransomware and password management.

3 Refer to Appendix B for further information on our sample selection.

Users who do not receive periodic training on cybersecurity could unintentionally expose online bank accounts to malicious software, thereby placing District assets at greater risk for unauthorized access, misuse or loss. Conducting online banking on a dedicated computer and providing periodic training to online banking users can help reduce the chances of a system compromise.

What Do We Recommend?

The Board should:

1. Adopt an online banking policy that describes authorized online banking activities and procedures for authorizing, processing and reviewing online banking transactions.

District officials should:

2. Establish sufficient written agreements with all banks in compliance with GML,[4] and ensure those who perform online banking transactions are familiar with their content.
3. Establish online banking procedures that adequately segregate duties, so that one individual cannot perform all phases of online banking transactions, or establish mitigating monitoring procedures.
4. Dedicate a computer workstation for the sole purpose of performing online banking transactions.
5. Provide periodic Internet security awareness training to all employees who conduct online banking.

4 See supra, note 1.

Appendix A: Response From District Officials

Huntington Union Free School District
James W. Polansky | Superintendent of Schools
P.O. Box 1500 • Huntington, NY 11743
Phone (631) 673-2038
Fax (631) 423-3447
jpolansky@hufsd.edu

January 11, 2023

Mr. Ira McCracken, Chief Examiner
Division of Local Government & School Accountability
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
(Muni-Hauppauge@osc.ny.gov)

Office of the New York State Comptroller
Division of Local Government & School Accountability
PSU – CAP Submission
110 State Street, 12th Floor
Albany, NY 12236
(caps@osc.state.ny.us)

Unit Name: Huntington Union Free School District
Audit Report Title: Online Banking
Audit Report Number: *2022M-178*

Dear Mr. McCracken:

The Huntington School District is in receipt of report *2022M-178*, issued following the recent audit conducted by examiners from the State Comptroller's office. On behalf of the Board of Education and district administration, I'd like to thank the examiners for their time, effort, guidance and professionalism in reviewing the district's processes and internal controls related to online banking. In that the suggestions made by the examiners have either already been implemented or are near implementation as documented within the report, please allow this correspondence to serve as both the district's response and correction action plan.

We appreciate acknowledgement of the fact that all online banking transactions within the district were made appropriately and for legitimate purposes, as well as recognition of the ongoing efforts of our business office staff in this regard. In addition, we appreciate the opportunity to strengthen our internal controls and further the district's cybersecurity efforts during a time when such risks have never been higher.

Audit Recommendation 1: Adopt an online banking policy that describes authorized online banking activities and procedures for authorizing, processing and reviewing online banking transactions.

Plan of Action: The Huntington Board of Education has adopted a dedicated online banking policy (Board Policy 5515), which incorporates all recommended provisions.

Implementation Date: January 9, 2023 (date of formal adoption)

Person(s) Responsible: Assistant Superintendent of Finance & Management Services, Superintendent of Schools, Board of Education

Audit Recommendation 2: Establish sufficient written agreements with all banks in compliance with GML and ensure those who perform online banking transactions are familiar with their content.

Plan of Action: Enter into formal agreements with two banks wherein the district maintains accounts and performs banking transactions that follow General Municipal Law and address electronic or wire transfers. Bank #1 maintains accounts for over 300 school districts but did not offer its clients an agreement that follows General Municipal Law and addresses electronic or wire transfers. The District has actively been working Bank #1 and the bank's legal department to develop an agreement as outlined in the Local Government Management guide.

Implementation Date for Bank #1: March 1, 2023 or as soon as new agreement is finalized.

Implementation Date for Bank #2: Pertinent agreement executed on September 28, 2022

Person(s) Responsible: Assistant Superintendent of Finance & Management Services

A Tradition of Excellence since 1657

Audit Recommendation 3: Establish online banking procedures that adequately segregate duties, so that one individual cannot perform all phases of online banking transactions, or establish mitigating monitoring procedures.

Plan of Action: The district has developed procedures ensuring that no one individual will have system rights to create and authorize any electronic fund transfer. The District Treasurer will be assigned 'creation rights' for electronic fund transfers, as appropriate. A second individual (Business Official or Accountant) will be assigned rights to authorize or release a wire transfer, ACH or other electronic transfer of funds.

Implementation Date: New procedures implemented November 1, 2022

Person(s) Responsible: Assistant Superintendent of Finance & Management Services

Audit Recommendation 4: Dedicate a computer workstation for the sole purpose of performing online banking transactions.

Plan of Action: A dedicated computer has been installed in the District treasurer's office for the sole purpose of performing online banking transactions.

Implementation Date: Installation completed on October 14, 2022

Person(s) Responsible: Assistant Superintendent of Finance & Management Services

Audit Recommendation 5: Provide periodic Internet security awareness training to all employees who conduct online banking.

Plan of Action: Management had already developed an annual Internet security awareness training program and has additionally contracted [redacted] to provide supplemental training, as needed, throughout each year.

Implementation Date: Training was provided to the cited individuals on August 19 and 26, 2022.

Person(s) Responsible: Assistant Superintendent of Finance & Management Services

Please do not hesitate to contact me should you have any further questions.

Yours truly,

James W. Polansky
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, our audit procedures included the following:

- We interviewed District and bank officials to obtain an understanding of the District's online banking practices and determine whether District officials who were involved in online banking activities received Internet security and awareness training.
- We reviewed the District's agreements with its banking institutions to determine whether the District entered into adequate written agreements. We also reviewed District policies and procedures to determine whether the Board adopted an adequate online banking policy.
- We observed online banking access from login to logout and reviewed user permissions reports for officials who were involved in online banking transactions.
- We examined the computers used to perform online banking activities, exported their website browsing histories, using a computerized exporter script, and reviewed the browsing histories.
- Officials recorded 508 online banking transactions, which consisted of electronic payments and transfers totaling $299,778,818, during our 23-month audit period. We used our professional judgement to select and test six of the 23 months. These six months consisted of two periods of three consecutive months during each school year in our audit period. Because the three-month periods occurred in different fiscal years, and at different times of each fiscal year, we deemed this sufficient for audit testing.
- During our six-month sample, officials recorded 201 transactions totaling $176,783,291, which consisted of 98 online payments and 103 transfers. We reviewed these transactions to determine whether all transfers occurred between District bank accounts. We also reviewed supporting documentation for the external wire transfers and ACH payments to determine whether the transactions were for appropriate District purposes.

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

HAUPPAUGE REGIONAL OFFICE – Ira McCracken, Chief of Municipal Audits

NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533

Tel (631) 952-6534 • Fax (631) 952-6091 • Email: Muni-Hauppauge@osc.ny.gov

Serving: Nassau, Suffolk counties