New York State Comptroller
THOMAS P. DiNAPOLI

North Babylon Union Free School District

Online Banking

2023M-156 | June 2024

Division of Local Government and School Accountability

Contents

Report Highlights

North Babylon Union Free School District

Audit Objective

Determine whether North Babylon Union Free School District (District) officials ensured online banking transactions were appropriate and secure.

Key Findings

While we determined that online banking transactions were appropriate, the Board of Education (Board) and District officials did not meet all the requirements of New York State General Municipal Law (GML) Section 5-a and must improve controls over online banking to ensure these transactions are secure. In addition to sensitive information technology (IT) control weaknesses that we confidentially communicated to District officials, we found that:

- District officials did not enter into an adequate written bank agreement with their banking institution, and the Board did not adopt an online banking policy.
- Employees who performed online banking activities did not receive cybersecurity awareness training.
- The District's acceptable use policy (AUP) was insufficient and not communicated to employees who performed online banking transactions.

Key Recommendations

- Enter into an adequate written bank agreement with their banking institution and adopt an online banking policy.
- Provide periodic cybersecurity awareness training and an updated AUP to employees who perform online banking transactions.

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

Audit Period

July 1, 2021 – April 11, 2023

Background

The District serves the Town of Babylon in Suffolk County and is governed by an elected seven-member Board responsible for managing and controlling the District's financial and educational affairs. The Superintendent of Schools is the 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 Board-appointed Treasurer and Deputy Treasurer are responsible for performing online banking transactions, and the Assistant Superintendent for Business (ASB) is responsible for overseeing these transactions. The Director of Student Data Services (IT Director) is responsible for ensuring staff receive cybersecurity awareness training and are informed about IT policies.

Quick Facts	
Total Online Banking Transactions During Audit Period	$338.9 million
Total Electronic Transfers Reviewed	$92.8 million
Authorized Online Banking Users During Audit Period	8

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 should establish adequate controls to ensure online banking transactions are for appropriate district purposes and secure.

How Should a Board and District Officials Ensure Online Banking Transactions Are Appropriate and Secure?

GML Section 5-a allows districts to disburse or transfer funds using an electronic funds transfer (EFT), provided that the governing board enters into a written agreement with the bank. An EFT is the electronic transfer of money from one bank account to another, either within a single bank or between multiple banks, through computer-based systems without the direct intervention of bank staff. A bank agreement must describe the way 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.

To help ensure online banking transactions are appropriate and secure, a board and district officials should implement online banking security procedures that include 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 procedures to monitor and control online banking transactions. The policy should:

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

A board and district officials should develop and adopt an AUP to inform users, including those responsible for performing online banking transactions, about appropriate and safe computer use, along with expectations concerning personal use of IT equipment and user privacy. The AUP should be communicated to all employees and other individuals (e.g., consultants, vendors) who utilize the District's computers, Internet and email to perform their job duties, and all users should acknowledge that they understand and will abide by the policy.

Employees should not be permitted to perform online banking activities until they receive sufficient, relevant cybersecurity awareness training on safe computing

practices. Cybersecurity awareness training could include communication of the district's online banking policy and procedures; discussion of new scams that are being used to steal banking information; social engineering reminders; and other online banking security-related matters. Internet browsing could cause district computers to become infected with malicious software that may compromise any personal, private, or sensitive information (PPSI)[1] residing on them. Exposure to malware could be minimized by using a separate, dedicated computer (one that is not used for email or Internet browsing) for online banking activities, if possible. A dedicated computer that is restricted from email access and Internet activity other than online banking is less likely to encounter malware.

In lieu of a dedicated computer, district officials could implement mitigating controls to reduce online banking risks introduced by malware. Such mitigating controls could include, but are not limited to, ensuring that computers are secured with user accounts and passwords that meet industry standards, online banking activities are not performed while logged into user accounts with local administrative access, and antivirus protection and patches are up-to-date.

The Board and District Officials Should Improve Controls Over Online Banking Transactions to Ensure They Are Secure

The District maintained 14 bank accounts with online transfer capabilities at one bank. The ASB, Treasurer and Deputy Treasurer had the ability to transfer money online between bank accounts (intra-bank), initiate online wire transfers (to other financial institutions), and create and edit templates for repeat transactions. The payroll clerk could only upload payroll information required by the bank to execute Automated Clearing House payments, and the Director of Food Services had read-only access to the lunch bank account. All five current online bank users entered their own username and password, along with a security token password, to access the online banking system.

Bank Agreement and Online Banking Policy – The District had a written bank agreement, referred to as the "Authorization and Agreement for Treasury Management Services," that was signed by the former Treasurer in September 2020. This agreement, together with the "General Provisions" and "Service Terms" of each banking service enrolled by the District and any corresponding "Operational Instructions," collectively made up the "Treasury Management Terms and Conditions Agreement" (Agreement).

The Agreement described the manner in which bank account and wire transfers could be accomplished but did not identify the bank account names or numbers

1 PPSI is any information to which unauthorized access, disclosure, modification, destruction – or disruption of access or use – could have or cause a severe impact on critical functions, employees, students, third-parties or other individuals or entities.

from which electronic transfers could be made, or the District employees who were authorized to request an electronic transfer of funds. Furthermore, the Agreement did not address security procedures to verify that payment orders were for District purposes or reviewed to detect errors in transmission or content. The "General Provisions" stated that the District could use the bank's online banking services in accordance with any security procedures set forth in the applicable "Operational Instructions." The District did not have a copy of the "Operational Instructions" on file and although we requested a copy from bank officials, they were not provided to the audit team. Therefore, we could not verify whether the "Operational Instructions" contained the information that was lacking in the other documents that made up the Agreement, such as identifying names and numbers of bank accounts from which transfers may be made, the individuals authorized to request transfers and security procedures to verify that payment orders are legitimate. Without an adequate online bank agreement, District officials cannot ensure that only authorized employees are performing online banking transactions and District employees understand their roles when performing these transactions, increasing the risk that inappropriate transactions and errors may occur and remain undetected.

Additionally, the Board did not adopt an online banking policy that describes the online activities that District employees were authorized to perform; identifies which employees were authorized to process transactions; specifies which devices to use and their locations; establishes an approval process to verify the accuracy and legitimacy of transfer requests; requires authorized employees to review and reconcile transfers; or establishes procedures when responding to fraudulent activity.

We reviewed 123 online banking transactions totaling $92.8 million, including 75 intra-bank transfers ($67.8 million) and 48 wire transfers ($25 million), and determined that all transactions were for appropriate District purposes, adequately supported, and made between authorized accounts or with approved external recipients. However, without an online banking policy and an adequate written agreement with their banking institution, the District had an increased risk that inappropriate transactions or errors could occur and remain undetected.

Acceptable Use Policy – The District's AUP stated that all users of the District's computer system (DCS) are subject to the policy and accompanying regulations. The Superintendent or designee(s) were directed to provide staff with training in the proper and effective use of the DCS. The AUP further stated that staff use of the DCS was conditioned upon a written agreement with the staff member to be kept on file in the District's office. The AUP also said, "This policy does not attempt to articulate all required or acceptable uses; nor is it the intention of this policy to define all inappropriate usage. Administrative regulations will further define general guidelines of conduct and use."

District officials could not determine who at the District was responsible for disseminating the AUP to staff. As a result, the AUP was not effectively communicated to staff and District officials did not ensure that the staff had a written agreement for use of the DCS which was kept on file in the District's office, as required by the AUP. As a result of our inquiries, the IT Director sent an online questionnaire to teaching staff in August 2023 that included a link to the AUP and an acknowledgment that they have read and agree to its terms. The IT Director told us he is working to provide the link to the AUP and acknowledgment to all staff.

The AUP did not provide guidance to employees describing acceptable computer use, including web browsing and other personal use of assigned computers. Because the AUP was not properly communicated to employees and lacked necessary guidance, there was an increased risk of unauthorized access to or compromise of the District's online banking service. For example, some websites may be malicious or contain code to compromise a user's computer or prompt the user to perform activities that result in malware infection. The AUP should dissuade employees from visiting websites and downloading software or files from unknown or untrusted sources, as these actions increase the likelihood of computers being exposed to malware. The IT Director agreed that it should be his responsibility to develop administrative procedures for acceptable computer use because it is an IT policy; however, he was not designated to develop these procedures by the Superintendent, who left the District shortly before we began our fieldwork.

Dedicated Computer and Cybersecurity Training – District officials did not use a dedicated computer to process online banking transactions. Instead, the five current authorized users accessed the online banking software application from their assigned District computers. However, these employees all used their computers for other work-related activities, including connecting to the Internet and accessing email.

We examined the web browsing history for each user computer and determined that these employees used the computers to conduct their assigned District duties and other incidental uses. Unless mitigating controls are implemented, authorized users should access online bank accounts from one computer dedicated for online banking to help minimize exposure to malicious software.

Seven of the eight employees who had access to the District's online banking system during the audit period (including a former Treasurer and two former payroll clerks) did not receive cybersecurity awareness training as required by the AUP. The Director of Food Services was the only employee who received cybersecurity awareness training. The ASB, Treasurer, Deputy Treasurer and payroll clerk took the training in March 2023 after we brought the issue to their attention.

The IT Director, who is responsible for providing cybersecurity awareness training to District employees, said that he mistakenly did not include the business office user group in the cybersecurity awareness training campaign, which is why the seven employees did not receive the training. District employees, including those with access to perform online banking functions, who do not receive periodic training on cybersecurity, could unintentionally expose the computers 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 to ensure that employees are aware of their responsibilities and that clearly describes the online banking activities and procedures for authorizing, processing and reviewing online banking transactions.

2. Amend the written bank agreement to be in compliance with GML and ensure it is on file at the District.

The IT Director and District officials should:

3. Ensure there is a sufficient written bank agreement in compliance with GML and on file at the District.

4. Update the AUP to include administrative regulations that provide guidance to employees about acceptable web browsing and personal use of computers, disseminate the AUP to all employees, and collect employee acknowledgements of the AUP.

5. Provide periodic cybersecurity awareness training to all employees who conduct online banking transactions.

6. Consider dedicating one computer to be used for the sole purpose of performing all online banking transactions or implement mitigating controls.

Appendix A: Response From District Officials

NORTH BABYLON SCHOOL DISTRICT

North Babylon Schools
5 Jardine Place, North Babylon, NY 11703
T: 631-620-7002 | F: 631-321-3295 | www.northbabylonschools.net

Kenneth E. Graham, Ed.D.
Superintendent of Schools

May 21, 2024

Mr. Ira McCracken, Chief of Municipal Audits
Division of Local Government and School Accountability
Office of the New York State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533

Dear Mr. McCracken,

The North Babylon Union Free School District has recently received the draft *Report of Examination - Online Banking* (2023M-156) issued by the Office of the New York State Comptroller, which covered the period from July 1, 2021 through April 11, 2023. We are pleased to note the acknowledgement that all online banking transactions examined during the audit period were adequately supported and appropriate for District operations and objectives.

We appreciate the findings and recommendations outlined in your draft report and are in agreement with them. As a District, we are committed to implementing these recommendations to further reinforce our internal control structure over financial oversight and operations. As of the date of this correspondence, some of the recommendations outlined in the report have already been implemented or will be implemented in the near future. The District's detailed corrective action plan will be provided separately at a later date.

On behalf of the Board of Education and District Administration, we extend our gratitude to your office and the examiners involved in this engagement. Their hard work, dedication, professionalism and guidance has been greatly appreciated.

Sincerely,

Kenneth E. Graham, Ed.D.
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. We obtained an understanding of internal controls that we deemed significant within the context of the audit objective and assessed those controls. Information related to the scope of our work on internal controls, as well as the work performed in our audit procedures to achieve the audit objective and obtain valid audit evidence, included the following:

- We interviewed District employees and bank officials to obtain an understanding of the District's online banking practices and determine whether employees involved in online banking activities received cybersecurity awareness training.
- We reviewed District policies and procedures to determine whether the Board adopted an adequate online banking policy and IT acceptable use policy.
- We reviewed the District's written agreement with its banking institution to determine whether the agreement was adequate. We reviewed the written bank agreement signed by the District's former Treasurer in September 2020. We reviewed the "General Provisions" and "Service Terms" for each banking service enrolled in by the District. The corresponding "Operational Instructions" were not available for our review.
- We reviewed banking user permission reports for the eight employees involved in online banking during the audit period, including the ASB, the Director of Food Services, the current and former Treasurer, the Deputy Treasurer, and the current and two former payroll clerks, to determine the bank accounts they can access and the transactions they can perform.
- On March 23, 2023, we ran a computerized audit script to export the web history files from the five computers assigned to online banking users. We examined the exported web history data for indications of personal Internet use.
- We used our professional judgment to select a sample of the three months in our audit period with the largest dollar amount of online banking transactions. We tested 123 transactions totaling $92.8 million, including 75 intra-bank transfers ($67.8 million) and 48 wire transfers ($25 million), to determine whether all transfers occurred between authorized District bank accounts and all wires were sent to authorized external accounts/recipients. We reviewed supporting documentation for these transfers to determine whether the transactions were for appropriate District purposes.

Our audit also examined the adequacy of certain 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 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.ny.gov/files/local-government/pdf/regional-directory.pdf

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

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.ny.gov/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.ny.gov/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.ny.gov/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.ny.gov/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.ny.gov/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.ny.gov/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.ny.gov/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

https://www.osc.ny.gov/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