OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Controls Over Online Banking in School Districts

2010-MS-11

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

February 2011

Dear School District Officials:

A top priority of the Office of the State Comptroller is to help local government officials manage government resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of local governments statewide, as well as compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations and school district governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard local government assets.

Following is a report of our audit titled Controls Over Online Banking in School Districts. This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the General Municipal Law.

This audit's results and recommendations are resources for school district officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

Office of the State Comptroller
Division of Local Government
and School Accountability

State of New York
Office of the State Comptroller

EXECUTIVE SUMMARY

Online banking allows the convenience of moving money between bank accounts,[1] reviewing transaction histories, reconciling accounts at any time, and closely monitoring cash balances for more effective investing. Local governments, including school districts, are authorized[2] to disburse or transfer funds in their custody by means of electronic or wire transfers. In a school district, certain business personnel are generally authorized to perform transfer transactions on the district's online banking website. School districts use internal controls and technology controls to ensure that transactions are authorized and that computers used to access banking websites are properly protected.

Recently, there has been a significant increase in fraud involving the exploitation of valid online banking credentials that can result in fraudulent electronic cash transfers of district funds to bank accounts in the United States or foreign countries. Recently, two New York State school districts[3] were targets of cyber fraud, and initially lost a total of $4.4 million as a result of these thefts. To date, the districts have recovered all but $497,200 of the amounts stolen. Having good controls over online banking process and computer usage, specifically Internet usage, can reduce the risk of fraud involving the exploitation of school district bank accounts. Our audit examined controls over the online banking transactions at the Greater Amsterdam, Highland Falls-Fort Montgomery, Longwood, Marcellus, Oneonta and South Colonie School Districts. These six districts' collective cash balance as of June 30, 2010 was almost $110 million.

Scope and Objective

The objective of our audit was to determine whether school districts adequately controlled online banking activities for the period July 1, 2009 to October 31, 2010. Our audit addressed the following related question:

- Have school districts established adequate controls over their online banking transactions?

[1] Examples include a transfer from the general fund money market account to the general fund checking account to pay vendor claims, or a transfer from the trust and agency fund account to the payroll fund account to cover payroll expenses.

[2] General Municipal Law, Section 5-a

[3] The Lindenhurst Union Free School District had recovered all fraudulently transferred funds, totaling $601,577, as of May 2008. The Duanesburg Central School District has recovered $2.5 million of the $3.8 million targeted by cyber theft (an improper transfer of $759,000 was initiated but not sent by the bank). The District is still seeking recovery of the remaining $497,200.

Audit Results

We found that school districts can improve controls over their online banking processes. Our tests of 1,817 online transfers at these six districts found that all the transfers were appropriate and properly recorded. However, we also identified risks in online processing activities at all the districts. For example, while we found varying levels of online banking controls in place at all six districts, five districts lacked a comprehensive online banking policy that clearly describes each district's online banking activities, identifies the employees who are authorized to perform them, and provides for verification of the accuracy and legitimacy of transfer transactions. We found that each district had properly segregated the critical duties of initiating, authorizing and recording online fund transfers; however, we also found that four districts allowed employees to perform online transfers from non-district computers that are not subject to district security protections. Unless districts strengthen their controls over online banking processes and regularly review the effectiveness of these controls, district funds will be at increased risk of being stolen through cyber fraud activities.

It is also important that districts maintain adequate information technology controls that protect district computers from malicious software and allow access to district-approved websites. We found that one district lacked controls that help ensure employees access the internet in a safe and appropriate manner. Without adequate technology controls, district computers can be vulnerable to viruses and intrusions that can result in theft of district funds.

Comments of District Officials

The results of our audit and recommendations have been discussed with school district officials and their comments, which appear in Appendix A, have been considered in preparing this report.

Introduction

Background

Most banking institutions offer some type of online banking service for their customers. Online banking allows the convenience of moving money between bank accounts, reviewing transaction histories, reconciling accounts at any time, and closely monitoring cash balances for more effective investing. School districts are allowed to disburse or transfer funds in their custody by means of electronic or wire transfer.

Generally, business office staff are responsible for online banking transactions and processes. Wire transfers are often used for distributing payroll via direct deposit, for paying Federal and State tax withholdings, for paying a district's share of State retirement contributions, and for paying retirement plan contributions. Intra-bank transfers are generally used for transferring district money from one fund's bank account to another (e.g., the transfer of money from the trust and agency fund to the general fund for the bi-weekly payroll).

To initiate an online banking transaction,[4] a district follows bank procedures to assign user rights to staff involved in the online banking process. Users log onto the online banking website with a unique username and password. One user initiates the transfer by entering the data on the online banking website while a second user typically authorizes or releases[5] the funds to their destination. The bank usually provides the district with a confirmation record and the district keeps this record on file with other transfer documentation. One of the users or another staff member enters the transfer data into the district's accounting system.

Because connecting to the Internet is a necessary part of the online banking process, districts must recognize and anticipate vulnerabilities inherent in online activities. Poor controls over online banking increase the risk that an entity may become the victim of cyber fraud and experience financial losses that may not be recoverable.

[4] Online transactions include the transfer of money from a district account to a non-district account (wires) and the transfer of money from one district account to another (intra-bank transfers).

[5] A transfer between district accounts usually does not require district personnel to authorize or release the transaction because money is not leaving the district's possession.

There has been a significant increase in fraud involving the exploitation of valid online banking credentials. Online banking fraud typically originates through fake email messages or malicious software (malware). The targeted user may receive an email that either contains an infected attachment or directs the recipient to an infected website. Once the recipient opens the attachment or visits the website, malware containing a key logger (which captures the user's keystrokes) is installed on the user's computer. The key logger harvests log-in information that allows the perpetrator to masquerade as the legitimate user or creates another user account. Thereafter, fraudulent electronic cash transfers are initiated and directed to bank accounts in the United States or foreign countries.

For example, the Lindenhurst Union Free School District was a victim of cyber theft. Our audit[6] found that, during a four business-day period, six unauthorized transfers totaling $601,577 were initiated that improperly transmitted money from the District's general fund account to various non-District bank accounts. The bank notified the District of these transactions and was able to recover five transfers totaling $496,590. The district recovered the balance of $104,987 in May 2008 from its insurer and the bank. According to media reports, the Duanesburg Central School District was targeted in a series of online attempts to steal $3.8 million in District funds over a three business-day period. Bank officials notified the District of an attempted transfer of $758,758 from a District account to an overseas account, and also noticed other suspicious transfers in the two previous days. Although the bank was able to recover about $2.5 million, the remaining $497,200 in District funds had not been recovered at the time of the media report in February 2010.

Good controls over computer usage, specifically Internet usage, reduce the risk of fraud involving the exploitation of school district bank accounts. Our audit examined six school districts from across the State[7] to assess their internal controls over online banking transactions. The following table provides background information on each school district.

[6] The report on the Lindenhurst Union Free School District, entitled Internal Controls Over Selected Financial Operations (2009M-155), was released on February 5, 2010.

[7] We judgmentally selected these six school districts to obtain a geographically diverse sample of districts that were medium to large in size, based on enrollment data.

BACKGROUND FOR EACH SCHOOL DISTRICT AUDITED			
School District	**Cash Balance on June 30, 2010 (in Millions)**	**Annual Expenditures 2009-2010 (in Millions)**	**Enrollment 2009-2010**
Greater Amsterdam CSD	$24.8	$51.8	3,700
Highland Falls-Fort Montgomery CSD	$3.0	$22.8	1,110
Longwood CSD	$57.0	$187.3	9,110
Marcellus CSD	$5.0	$28.7	2,000
Oneonta CSD	$3.1	$32.7	1,880
South Colonie CSD	$16.8	$84.3	5,400
Total	**$109.7**	**$407.6**	**23,200**

Objective

The objective of our audit was to determine whether school districts adequately controlled online banking activities. Our audit addressed the following related question:

- Have school districts established adequate controls over their online banking transactions?

Scope and Methodology

We examined the internal controls of the online banking processes of six school districts for the period July 1, 2009 to October 31, 2010.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit is included in Appendix B of this report.

Comments of District Officials

The results of our audit and recommendations have been discussed with districts officials and their comments, which are included in Appendix A, have been considered in preparing this report.

Controls Over Online Banking

District officials are responsible for adequately safeguarding district assets, including funds that are transferred from one district account to another, or to non-district accounts, through online banking processes. Our tests of 1,817 online transfers at these six districts found that all the transfers were appropriate and properly recorded. However, we also identified risks in online processing activities at all the districts. For example, while we found varying levels of online banking controls in place at all six districts, five districts lacked a comprehensive online banking policy that clearly describes each district's online banking activities, identifies the employees who are authorized to perform them, and provides for verification of the accuracy and legitimacy of transfer transactions. Although each district had properly segregated the critical duties of initiating, authorizing and recording online fund transfers, four districts allowed employees to perform online transfers from non-district computers that are not subject to district security protections. Unless districts strengthen their controls over online banking processes and regularly review the effectiveness of these controls, district funds will be at increased risk of being stolen through cyber fraud activities.

It is also important that districts maintain adequate information technology controls that protect district computers from malicious software and allow access to district-approved websites. We found that one district lacked controls that help ensure employees access the Internet in a safe and appropriate manner. Without adequate technology controls, district computers can be vulnerable to viruses and intrusions that can result in theft of district funds.

Internal Controls

Internal controls over online banking activities consist of detailed policy guidance to direct employee online activities, properly segregated financial duties, and controls that prevent access to district banking websites from other than district-owned computers. We found that five districts (Highland Falls-Fort Montgomery, Longwood, Marcellus, Oneonta, and South Colonie) lacked a comprehensive policy regarding the online banking process. Further, four of the six districts (Amsterdam, Highland Falls-Fort Montgomery, Marcellus, and Oneonta) allow users to access the banking websites from computers other than designated district computers. These control weaknesses put district assets at risk.

Policy Guidance — Effective internal controls over online banking include policies and procedures to properly monitor and control online banking transactions. A comprehensive online banking policy clearly describes the online banking activities the district will engage in, specifies which district employees have the authority to process transactions, establishes a detailed approval process to verify the accuracy and legitimacy of transfer requests, and requires a monthly report of all online banking transactions. It is important that someone independent of the online banking process review this report and reconcile it with the monthly bank statement to verify that all transactions were properly approved and appropriate.

We found that only one district (Amsterdam) had Board-adopted policy guidance in place for online banking activity. Although the remaining districts generally have processes in place to provide for controls over online transfers, these districts can strengthen existing controls by adopting comprehensive policy guidance that addresses all aspects of online banking operations. District officials should review this policy guidance on a regular basis to ensure it remains current and effective.

Segregation of Duties — Good management practices include establishing proper segregation of duties over the online banking processes so that no one individual controls all phases of a transaction. In general, the functions of transaction approval, record keeping, and asset custody must be separated. The authorization and transmitting functions should be segregated and, if possible, the recording function should be delegated to someone who does not have either approval or transmitting duties. The primary purpose of segregating duties is to prevent or detect errors and fraudulent activity in a timely manner. If it is not practicable to adequately segregate these duties, district officials should implement mitigating controls, such as increased management review.

We found that the six districts have adequately segregated, conflicting duties in online banking activity by dividing tasks among multiple employees, ensuring that proper authorization steps are followed, and by providing for sufficient compensating controls, as necessary. For example, in South Colonie, the Assistant Superintendent and the Business Manager have access to the online banking website to perform their authorized duties. To initiate a transaction, the Business Manager enters data from source documents into the online banking website and prints out a record of the transfer. This record is given to the Assistant

Superintendent who reviews the data and signs off on the record for approval. Bank reconciliations are performed by the Assistant Superintendent's Secretary who is independent of the online banking process. The bank reconciliations are included in the Treasurer's report submitted to and reviewed by the Board monthly. Highland Falls-Fort Montgomery, Amsterdam, Longwood, Marcellus and Oneonta used similar procedures to segregate critical duties for initiating, authorizing and reconciling online banking transactions.

We reviewed online banking transactions for a three-month period at each district to determine whether transactions were properly recorded, appropriate, and complied with policies. We tested 1,817 transfers made between July 1, 2009 and October 31, 2010, totaling $302 million. Of the 1,817 transactions, 1,262 transfers totaling $170.5 million were between district accounts; the other 555 transfers totaling $131.5 million were made from district to non-district accounts. The transfers between district accounts were mostly for biweekly payroll transactions and for vendor check payments made from the general fund. We found that all transfers between district accounts were accurate, and that transactions were accurately recorded. We also found that transfers from district to non-district accounts were appropriate and proper. Although our limited tests did not identify any incorrect or inappropriate transactions, it is essential that school districts segregate online banking duties to reduce the risk that errors could occur or funds could be diverted without detection.

Authorized Access — Good management practices would not only limit the users authorized to execute online banking activities, but also limit the computers on which the activity can take place. Authorized online banking users should be able to access district bank accounts from only the district computer designated for online banking transactions. Non-district computers may not have the same security protections as district computers, and transactions executed from those computers could be more at risk. Authorized users should be assigned user names, passwords, and token identifications[8] that are user-specific and maintained in a secure place. By prohibiting access to the district's online banking website from non-district computers, districts can reduce the risk of theft by online hackers.

We found that only Longwood and South Colonie prevented users from accessing the banking websites from computers other than the

[8] Token identifications contain a number series assigned to a specific user.

designated district computer. These two districts give authorized personnel user names, passwords, and token identifications that must be used on the district computers designated for online banking. The token identifications are locked at the districts to prevent users from accessing the online banking websites from non-district computers. Unless districts officials restrict online banking to designated district computers, district funds are at risk of being stolen.

Information Technology Controls

District officials are responsible for maintaining adequate controls over employee computer use of district computers, including ensuring that employees engage in appropriate activity on the Internet. These controls include enabling website filtering software that allows employees to access only district-approved websites, and performing careful monitoring of Internet access to ensure appropriate use. Without strict monitoring systems in place, inappropriate Internet usage could put district computers at risk, including those designated to access online banking websites.

We found that five of the six districts had adequate information technology controls in place to limit risks associated with online banking. Highland Falls-Fort Montgomery, Longwood, Marcellus, Oneonta and South Colonie all use software securities and website filtering software that identify and address vulnerabilities. In addition, these districts have a category list of non-allowed websites, and have enabled controls that prevent access to these sites by the users of district computers. These system controls ensure that users access the Internet for only appropriate use, and prevent harmful viruses and intrusions that infect district computers and make the funds in district accounts vulnerable to theft.

However, in Amsterdam, one of the computers used for online banking contained malware (malicious software) and evidence that the user had visited phishing[9] sites. Further, the Internet use patterns included visits to high-risk websites, including pornographic websites, which could significantly jeopardize the safety of District assets. The District has website filtering software, but it had failed to block or deny access to these high-risk sites. Accessing the District's online banking website with an infected computer, especially when the District's website

[9] Phishing refers to fraudulent attempts to gain sensitive or confidential information from a computer user by means that appear to be trustworthy.

filtering software is not effective, puts the almost $25 million[10] in the District's 21 bank accounts at risk for theft.

Recommendations

1. School districts should create and implement comprehensive written policies for online banking operations and regularly review them to ensure they remain current.

2. School districts should ensure that authorized users access district banking websites from only those district computers that are designated for online banking activity.

3. School districts should monitor computer usage and ensure that the website filtering software and information technology security procedures are in place and operating effectively to provide for safe online banking operations.

[10] As of June 30, 2010

APPENDIX A

RESPONSES FROM DISTRICT OFFICIALS

We provided a draft copy of this global report to each of the six school districts we audited and requested responses. We received response letters from each school district.

Overall, the districts were in agreement with the findings and recommendations in the report. The following comments were excerpted from the responses we received.

The Greater Amsterdam School District – "Of the six school district audited, Amsterdam was found to be the only district with a comprehensive online banking policy. Other school districts should consider instituting a policy as well."

Highland Falls-Fort Montgomery School District — "… we gained in knowledge and perspective from the audit, and we hope that the results will inform others about the importance of policy that communicates to key staff and enables management to make informed business decisions on risk, need, and cost."

Longwood Central School District — "The district is satisfied with the findings presented in the draft report."

Marcellus Central School District — "On behalf of the district we thank you for the time, effort and constructive feedback provided during the examination, the exit conference and the draft report. We acknowledge that the report points out areas of potential risk and we appreciate the opportunity to respond and act on those recommendations."

Oneonta City School District — "The District will set up a laptop to be used solely for online banking transactions…"

South Colonie Central School District — "…Thank you for performing this valuable service to the school districts."

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

During this audit to gain an understanding of the internal controls over the online banking process, we interviewed school district business officials, staff, and reviewed policies and/or procedures for the online banking process. We verified these controls by observing online banking transactions being performed by personnel. We determined if controls are proper based on good business practice. Through interviews we were also able to determine if online banking websites were accessed from computers (home and public) other than district computers.

To determine if computerized data is reliable, we examined the five major funds' (general, cafeteria, federal, trust and agency, and capital) cash accounts to determine that the cash amounts in the District's accounting system are equal to the cash amounts on the bank statements. We took the amounts from the bank statements and reconciliations and matched them to the amounts on the trial balances. Then we traced the trial balance amounts to the general ledger detailed account amounts. Finally we traced the general ledger detailed account amounts to the warrants, cash disbursement and receipt journals, journal entries and source documents.

To determine if online banking transactions are accurate and recorded properly, we reviewed every bank statement for our audit scope of July 1, 2009 to October 31, 2010 for any transaction that seemed out of the ordinary. From there we selected a three month period[11] and documented every online banking transaction from every fund account based on the bank statements. Confirmations were sent out to the banks to ensure that we had every bank account from each district. For transactions between district accounts, we traced the amounts being withdrawn from one account and deposited into another. We ensured that, for the three month period, the withdrawals equaled the deposits. For transactions where money is being transferred to non-district bank accounts, we traced the amounts to transfer confirmations from the bank, to journal entries, and to source documents such as vendor invoices and documentation.

We reviewed the computers used for online banking to ensure proper use and that functioning securities are in place. We interviewed district information technology personnel to gain an understanding of the securities used, to determine if computers are checked for vulnerabilities, and to determine if website filtering software blocks certain sites. Then we examined computer use policies to determine the guidance provided to district staff. Finally, we checked the computers to see if there is virus prevention software, if software is up-to-date, if proper software is installed and if computer (Internet) usage is proper. We examined temporary Internet files, cookies, history files, favorites files, and downloaded pictures, music and videos for content to determine proper computer usage.

We conducted our 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[11] For Amsterdam, we reviewed every online banking transaction for the audit scope because of the computer use content found on a district computer used for online banking

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
http://www.osc.state.ny.us/localgov/

APPENDIX D
OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

Steven J. Hancox, Deputy Comptroller

LOCAL REGIONAL OFFICE LISTING

ALBANY REGIONAL OFFICE
Kenneth Madej, Chief Examiner
Office of the State Comptroller
22 Computer Drive West
Albany, New York 12205-1695
(518) 438-0093 Fax (518) 438-0367
Email: Muni-Albany@osc.state.ny.us

Serving: Albany, Columbia, Dutchess, Greene, Schenectady, Ulster counties

BINGHAMTON REGIONAL OFFICE
Office of the State Comptroller
State Office Building, Room 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware, Otsego, Schoharie, Sullivan, Tioga, Tompkins counties

BUFFALO REGIONAL OFFICE
Robert Meller, Chief Examiner
Office of the State Comptroller
295 Main Street, Room 1050
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming counties

GLENS FALLS REGIONAL OFFICE
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

Serving: Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Warren, Washington counties

HAUPPAUGE REGIONAL OFFICE
Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau, Suffolk counties

NEWBURGH REGIONAL OFFICE
Christopher Ellis, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Orange, Putnam, Rockland, Westchester counties

ROCHESTER REGIONAL OFFICE
Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street – Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

Serving: Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

SYRACUSE REGIONAL OFFICE
Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence counties