Office of the New York State Comptroller

Division of Local Government
& School Accountability

Lindenhurst Union Free School District

Internal Controls Over Selected Financial Operations

Report of Examination

Period Covered:

July 1, 2007 — June 30, 2008

2009M-155

Thomas P. DiNapoli

Table of Contents

		Page
AUTHORITY LETTER		2
EXECUTIVE SUMMARY		3
INTRODUCTION		6
	Background	6
	Objective	6
	Scope and Methodology	7
	Comments of District Officials and Corrective Action	7
BUSINESS OFFICE		8
	Electronic Wire Transfers	8
	Cash Receipts	10
	Treasurer's Signature Disk	11
	Recommendations	12
CLAIMS PROCESSING		13
	Recommendations	15
PROFESSIONAL SERVICES		16
	Recommendation	16
INFORMATION TECHNOLOGY		17
	Recommendations	19
APPENDIX A	Response From District Officials	21
APPENDIX B	OSC Comments on the District's Response	29
APPENDIX C	Audit Methodology and Standards	30
APPENDIX D	How to Obtain Additional Copies of the Report	32
APPENDIX E	Local Regional Office Listing	33

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

February 2010

Dear School District Officials:

A top priority of the Office of the State Comptroller is to help school district officials manage their districts efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support district operations. The Comptroller oversees the fiscal affairs of districts statewide, as well as districts' 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 district operations and Board of Education governance. Audits also can identify strategies to reduce district costs and to strengthen controls intended to safeguard district assets.

Following is a report of our audit of the Lindenhurst Union Free School District, entitled Internal Controls Over Selected Financial Operations. 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 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

The Lindenhurst Union Free School District (District) is governed by the Board of Education (Board) which comprises nine elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer of the District and is responsible, along with other administrative staff, for the day-to-day management of the District under the direction of the Board.

There are nine schools in operation within the District, with approximately 7,000 students and 1,500 employees. The District's budgeted expenditures for the 2007-08 fiscal year were $127 million, which were funded primarily with State aid, real property taxes, and grants.

During July 2007, six unauthorized on-line wire transfers amounting to $601,577 were initiated that improperly transmitted money from a general fund bank account to various non-District accounts in other banks. In August 2009, we referred this matter to the Suffolk County District Attorney's Office for further investigation. The Suffolk County District Attorney's Office investigated this matter and found no evidence of criminal activity by District officials or employees.

Scope and Objective

The objective of our audit was to determine if the District's internal controls over selected financial operations are appropriately designed and operating effectively for the period July 1, 2007, to June 30, 2008. Our audit addressed the following related questions:

- Are internal controls over Business Office operations appropriately designed and operating effectively to adequately safeguard District assets?

- Are internal controls over claims processing appropriately designed to ensure that claims are adequately audited prior to payment and that payments are made only for appropriate District purposes?

- Are internal controls over the procurement of professional services appropriately designed and operating effectively?

- Are internal controls over the District's information technology system appropriately designed to protect electronic data?

Audit Results

The Board and District officials need to establish better policies and procedures over several aspects of the District's operations in order to better safeguard public funds. The Board did not establish policies and District officials did not develop procedures to sufficiently guide District personnel in performing their job duties. For example, there were no written procedures for the protection and use of electronic signatures or for the appropriate authorization and review of electronic banking transactions. Additionally, cash receipt duties were not properly segregated in the Business Office, and unauthorized wire transfers were not investigated. These control weaknesses place the District's cash assets at an increased risk of mismanagement, misuse, loss and theft.

In July 2007, someone improperly transferred approximately $600,000 from a District bank account to various external bank accounts. Officers at the depository bank recognized the inappropriate nature of these transactions and took action to recover the funds. However, they were only able to recover $496,590. The District lost nearly $105,000.[1] We found that the Board and District officials never investigated and determined how the unauthorized on-line wire transfers were enacted, and never informed law enforcement officials of this significant theft, because they were reportedly told that the bank had notified the Federal Bureau of Investigations. Although controls over on-line wire transfers were improved, the controls over wire transfers initiated by telephone and fax continue to be poor; therefore, the District is still susceptible to the loss of cash through unauthorized transfers.

The Board appointed a claims auditor to audit District claims. However, we found that only the claims paid from the general fund were being audited prior to payment. During our audit period, payments totaling $9.4 million made from the school lunch fund, the capital projects fund and the special aid fund were not subject to audit prior to payment. As a result, the District does not have adequate assurance that all payments are appropriate and necessary. Our review of 24 claims paid from the school lunch fund, the capital projects fund and the special aid fund totaling $804,487 identified concerns with ten of the payments totaling $42,091.

The District's purchasing policy does not require officials to solicit competitive proposals, such as requests for proposals (RFP), prior to issuing a contract with a professional service provider. The District generally uses past experience in selecting professionals rather than selecting professionals based on a competitive process. We found that payments made to eight professional service providers totaling $900,000 were procured without soliciting RFPs. The District's failure to solicit competition prior to procuring professional services increases the risk that these services were not obtained at the lowest possible price.

Finally, the District uses a financial accounting software package to process and maintain the District's financial transactions. District officials have not developed policies and procedures to protect critical financial data. User access rights are not properly established, remote access is not being monitored, audit trail logs are not being reviewed and the District does not have a formal disaster recovery plan. As a result, critical financial data is subject to an increased risk of loss or misuse.

[1] The loss was reported to the District's insurance company. In May 2008, the District received a check for $102,487 from their insurance company and $2,500 from the bank, which was the full amount of the loss.

Comments of District Officials

The results of our audit and recommendations have been discussed with District officials and their comments, which appear in Appendix A, have been considered in preparing this report. District officials generally agreed with our recommendations and indicated that they planned to take corrective action. Appendix B includes our comments on issues raised in the District's response letter.

Introduction

Background

The Lindenhurst Union Free School District (District) is located in the Town of Babylon, in Suffolk County. The District is governed by the Board of Education (Board) which comprises nine elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer of the District and is responsible, along with other administrative staff, for the day-to-day management of the District under the direction of the Board.

There are nine schools in operation within the District, with approximately 7,000 students and 1,500 employees. The District's budgeted expenditures for the 2007-08 fiscal year were $127 million, which were funded primarily with State aid, real property taxes, and grants.

The Assistant Superintendent for Business is responsible for overseeing the District's Business Office and supervises employees who maintain the District's financial accounting records and process the District's cash receipts, disbursements, and payroll. The purchasing agent is responsible for authorizing purchases, and the District Treasurer is responsible for receiving, disbursing, and holding District money. In addition, the Board appointed a claims auditor to assume the powers and duties of approving and denying claims against the District. The District uses a financial accounting software package (financial software) to process and maintain financial transactions.

Objective

The objective of our audit was to determine if the District's internal controls over selected financial operations are appropriately designed and operating effectively. Our audit addressed the following related questions:

- Are internal controls over Business Office operations appropriately designed and operating effectively to adequately safeguard District assets?

- Are internal controls over claims processing appropriately designed to ensure that claims are adequately audited prior to payment and that payments are made only for appropriate District purposes?

- Are internal controls over the procurement of professional services appropriately designed and operating effectively?

- Are internal controls over the District's information technology system appropriately designed to protect electronic data?

Scope and Methodology

We examined the District's internal controls over selected financial operations for the period July 1, 2007, to June 30, 2008.

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 are included in Appendix C of this report.

Comments of District Officials and Corrective Action

The results of our audit and recommendations have been discussed with District officials and their comments, which appear in Appendix A, have been considered in preparing this report. District officials generally agreed with our recommendations and indicated that they planned to take corrective action. Appendix B includes our comments on issues raised in the District's response letter

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of the General Municipal Law, Section 2116-a (3)(c) of the Education Law and Section 170.12 of the Regulations of the Commissioner of Education, 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, with a copy forwarded to 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 Board should make the CAP available for public review in the District Clerk's office.

Business Office

The Board and District officials are responsible for establishing a good system of internal controls to provide reasonable assurance that cash is safeguarded. An effective internal control system includes policies and procedures intended to provide reasonable assurance that cash transactions are properly initiated, accurately recorded, deposited intact in a timely manner, and are properly approved and documented. Control procedures include establishing authorization to execute transactions, security of signature discs, and adequate segregation of duties.

We found that the Board did not adequately safeguard the District's cash assets. The Board did not establish adequate policies and District officials did not develop procedures to guide District personnel in performing their job duties regarding the handling of cash. There were insufficient controls over wire transfers and inadequate protection of the Treasurer's signature disk. Additionally, cash receipt procedures were not properly segregated. These control weaknesses place the District's cash assets at an increased risk of mismanagement, misuse, loss and theft. For example, in July 2007, an individual[2] improperly removed $601,577 from District bank accounts by means of unauthorized wire transfers. Because of actions taken by the bank, most of the money was returned to District accounts within a few days. However, almost $105,000[3] was not returned. In addition, the unauthorized wire transfers were not investigated. Therefore, the Board and District officials cannot be assured that this will not happen again.

Electronic Wire Transfers

Electronic wire transfers of school district funds are usually effective within minutes of being executed. The Treasurer, as custodian of District funds, is normally the official responsible for authorizing wire transfers. Effective controls over the wire transfer process include written policies and procedures to guide personnel in performing online banking activities. Safeguards for initiating an electronic wire transfer include the use of a password to authorize the transfer verbally, hand delivering a letter of authorization to the bank with the transfer instructions, or sending a fax with the authorized signature and password. At least two individuals should be involved in each electronic transaction. The authorization and transmitting functions need to be segregated and, if possible, the recording function should

[2] District officials believe that this individual was not a District official or employee. However, officials never identified who made the inappropriate transfers.

[3] The loss was reported to the District's insurance company. In May 2008, the District received a check for $102,487 from their insurance company and $2,500 from the bank, which was the full amount of the loss.

also be delegated to someone who does not have either approval or transmitting duties.

During our audit period, the Board did not adopt written policies addressing banking transactions and District officials did not develop specific procedures for electronic wire transfers. District officials and employees initiated electronic wire transfers from various accounts maintained in six different banks. District funds were transferred to other District bank accounts as well as to external bank accounts. During the audit period, District officials and employees initiated 372 electronic wire transfers by fax, phone or internet totaling $330.5 million. With the exception of two banks, which required that someone other than the person who initiated the on-line wire transfer confirm the transfer, the principal account clerk was the only person initiating and confirming wire transfers initiated by telephone and fax. Therefore, many electronic wire transfers were performed without an independent review of the appropriateness of the transfer.

District officials informed us that between Monday, July 2, 2007, and Thursday, July 5, 2007, six unauthorized wire transfers amounting to $601,577 were initiated that improperly transmitted money from a general fund bank account to various non-District accounts in other banks. The transfers were in amounts that ranged from $79,593 to $149,818. The bank detected the unusual transfers and notified the principal account clerk at her home on Friday, July 6, 2007. Once the bank was informed that these transfers were improper, bank officials contacted the beneficiary banks in an attempt to recover the proceeds of the electronic wire transfers. The bank was only able to recover five transfers totaling $496,590; the remaining $104,987 transfer was not recovered. If the bank had not noticed the suspicious activity during the week of July 2, 2007, the District would not have identified the theft of funds until the following week because the bank normally sends confirmations of electronic wire transfers one week after the transfer is initiated.

In August 2009, we referred this matter to the Suffolk County District Attorney's Office for further investigation. The Suffolk County District Attorney's Office investigated this matter and found no evidence of criminal activity by District officials or employees.

On Monday, July 9, 2007, the former Assistant Superintendent for Business sent a memo to the Board notifying them of the incident and stated that, "at no time were any District employees involved with the unauthorized withdrawal transactions." This statement was made to the Board without any formal investigation being performed. The Board did not initiate an internal or external investigation of the fraudulent transactions, and did not notify law enforcement agencies

of the theft, because they were reportedly told that the bank had notified the Federal Bureau of Investigations. On August 14, 2007, the loss was reported to the District's insurance company, and on May 9, 2008, the District received a check for $102,487 from their insurance company. A few weeks later the District received the remaining $2,500 from the bank. According to District officials, the former Superintendent disclosed the theft to the public after they received the insurance recovery.

District officials told us that the unauthorized transfers occurred because someone outside the District was able to fraudulently obtain the information necessary to access District cash. They claimed that the principal account clerk was the victim of a fraudulent e-mail, which was designed to appear as a legitimate request from the bank where the District's general fund bank account was maintained. The e-mail requested information that would have permitted the recipient to access the District's account and initiate wire transfers of District money.

The Board and District officials have never undertaken a formal investigation of the unauthorized transfers and have not taken sufficient action to correct internal control deficiencies that were in place at the time of the transfers. More than one year after the unauthorized transfers were made, District officials did not have written policies and procedures governing the wire transfer process. Discussions with the principal account clerk and a review of available documentation disclosed that the clerk was still solely responsible for initiating and receiving confirmation of wire transfer activity for at least three depository banks. Because the Board and District officials never investigated and determined how the unauthorized transfers were enacted and because of poor controls over wire transfers, the District continues to be susceptible to the loss of cash through unauthorized transfers.

Cash Receipts

District officials are responsible for establishing controls so that no single individual handles all or most aspects of the cash receipt processes. It is important that the work of one employee is routinely verified in the course of another employee's regular duties. If it is not feasible for District officials to segregate incompatible duties, they must implement compensating controls. Compensating controls over the cash receipt processes could include random reviews to verify that cash receipts are properly recorded and deposited to District bank accounts. Assigning incompatible duties to the same individual with limited supervisory oversight increases the risk that errors and/or irregularities might occur and go undetected.

The District collected more than $2 million in fees in 2007-08 for adult education courses, tuition payments from other districts, retiree's health insurance payments, and building use fees. We found that the District does not have policies and procedures to adequately segregate cash receipt duties. The principal account clerk is responsible for all aspects of the cash receipt process including opening the mail, collecting cash, issuing duplicate cash receipt forms, recording cash receipts in the Treasurer's cash receipt log, and depositing all cash receipts. With these duties, the principal account clerk could misappropriate receipts and adjust the accounting records to conceal the misappropriation.

Because of the poor segregation of duties over cash receipts, we tested five deposits, totaling $136,475, comparing cash receipt records to deposit slips and bank statements. Although we found no exceptions, when one person controls all phases of a transaction, it significantly increases the risk that errors as well as fraud may occur and not be detected in a timely manner.

Treasurer's Signature Disk

The Treasurer is the custodian of all District moneys and has the authority to sign all checks on behalf of the District. When authorized by the Board, checks may be signed with a facsimile signature of the Treasurer. However, when such a facsimile signature is used by someone other than the Treasurer it must be affixed under the supervision and control of the Treasurer.

The Board did not establish formal policies and District officials did not establish procedures for the use of facsimile signatures. As a result, the Treasurer did not always supervise and control the use of his signature disk. The signature disk, containing the Treasurer's signature, is kept in a safe in the Business Office. Both the principal account clerk and the Assistant Business Administrator have the combination to the safe and, therefore, the ability to use the signature disk. Neither of these individuals were authorized District signatories. We found that the District's principal account clerk applied the Treasurer's signature to checks when the Treasurer was not present. However, we were unable to determine whether or not the Assistant Business Administrator used the signature disk to sign District checks during our audit period. The principal account clerk explained to us that she used the signature disk to sign checks because the District issues checks for payroll or accounts payable each week, while the Treasurer only works at the District one day each month.

Due to this control weakness, we examined 20 expenditures, totaling $143,332, that were made using the Treasurer's signature disk to determine whether they were valid District transactions, and found no irregularities. However, the absence of comprehensive policies

and procedures for the control and use of the signature disks, and the Treasurer's lack of control over the use of his signature disk, increases the risk that his signature could be used to generate checks that are not for legitimate District purposes.

Recommendations

1. The Board and District officials should investigate all thefts of District funds and the appropriate authorities should be notified.

2. The Board should adopt, and employees should adhere to, written policies for cash receipts and disbursements. These policies and procedures should include the following requirements:

    - Wire transfers should be reviewed and approved by someone other than the individual who initiated the transfer. This second individual should also receive the transfer confirmation from the bank.

    - Cash receipt procedures should be adequately segregated. The duties of opening the mail should be segregated from the duties of handling cash. In addition, the duties of recording cash receipts should be segregated from the duties of preparing and depositing cash.

    - The Treasurer should keep personal control and custody of his signature disk and directly oversee its use. Access to his signature disk should not be available to unauthorized individuals.

Claims Processing

The objectives of a good claims processing system are to ensure that the amounts claimed represent actual and necessary District expenses and that every claim contains enough supporting documentation to determine whether it complies with statutory requirements and District policies. An effective claims processing system would ensure that vendors are not overpaid, discounts are not lost, taxes are not paid unnecessarily and that payments are not made for goods and services not received.

Education Law requires that school districts audit each claim before it is paid. This function can be performed either by the Board or a claims auditor appointed by the Board. The fundamental elements of auditing claim vouchers include being familiar with legal requirements associated with purchases in a school district, ensuring that voucher packages are complete, determining whether claims are for actual and reasonable public expenditures, inquiring into specific areas to determine whether District personnel have followed correct procedures, and being alert to indications of theft, abuse, or misuse of the District's assets, or other unethical procedures. Without a thorough audit of each claim, there is an increased risk that the District will pay for inappropriate expenses.

The Board appointed a claims auditor to audit District claims. However, the claims auditor was only auditing the claims paid from the general fund prior to payment. The claims auditor did not audit payments made from the school lunch fund, the capital projects fund and the special aid fund until after the claims were already paid. As a result, the District does not have adequate assurance that all payments are appropriate and necessary. During our audit period, 91 claims, totaling approximately $2.1 million, were paid from the school lunch fund; 70 claims, totaling $3.7 million, were paid from the capital projects fund; and 1,015 claims, totaling $3.6 million, were paid from the special aid fund.

Due to the weakness in the claims audit process, we examined 24 claims paid from the school lunch fund, the capital projects fund and the special aid fund totaling $804,487. We found that five payments were issued to vendors without the proper supporting documentation, three purchases were made that were not in accordance with District policy, the District paid sales tax to one vendor and one claim was a questionable use of District funds. For example:

- Five claims, totaling $32,589, were paid without bills or invoices from the vendors to support the payments. For

example, the District paid a vendor $22,264 to provide learning and developmental disability services to students even though there was no invoice from the vendor listing the types of services provided or the fees charged. Because the District paid vendors without receiving claims that provided supporting documentation, there was no way to determine if the claims were legitimate District expenditures. However, the five claims did appear to be legitimate District charges.

- On January 18, 2008, a vendor was paid for kitchen equipment repairs which totaled $2,608 and included $207 of sales tax. School Districts are exempt from paying sales tax; therefore, sales tax should not have been paid to this vendor. Instead, the District should have provided the vendor with a sales tax exemption form.

- Three purchases, totaling $5,894, were made without the solicitation of competitive quotes as required by the District's purchasing policy. The purchases included $2,608 for kitchen equipment repairs, $2,012 for printing a catalogue, and $1,274 for the purchase of a sink. According to District policy, purchases greater than $500 require the solicitation of a minimum of three telephone, written or fax quotations.

- An office supply store was paid $1,000 for 10 $100 gift certificates on November 19, 2007. According to District officials, these gift certificates were issued to teachers, who were working on a special program, to cover the cost of supplies. Although the purchase order for this expenditure stated that the Board approved these gift certificates, we found that the purchase was not approved by the Board. There is no provision in Education Law permitting school districts to issue gift certificates to employees. All supplies required by teachers should be obtained in the same manner as other District purchases, after the issuance of a purchase order and the submission of an invoice or bill from the vendor showing the items purchased.

When claims are paid without being subject to audit, there is a significant risk that payments could be made in erroneous amounts, be based on insufficient documentation, or made for other than proper District purposes. The practice of not auditing the claims before checks are paid weakens the controls over the disbursements of funds and provides opportunities for individuals to perpetuate and conceal fraud. The failure of the claims auditor to audit all claims increases the risk that errors or irregularities could occur and remain undetected and uncorrected.

Recommendations

3. The Board should ensure that the claims auditor conducts a proper audit of all District claims in accordance with laws, regulations, and District policies.

4. The Board and District officials should ensure that claims are paid only after a thorough audit by the claims auditor.

Professional Services

Competitive bidding is not required for the procurement of professional services that involve specialized skill, training and expertise, use of professional judgment or discretion, and/or a high degree of creativity. General Municipal Law (GML) requires the District to adopt internal policies and procedures governing the procurement of goods and services when competitive bidding is not required. An effective and comprehensive purchasing policy should require the District to use competition whenever such services are needed. A request for proposal (RFP) process is one method that could help ensure that the District receives the desired service for the best price.

The District's purchasing policy does not require officials to solicit competitive proposals prior to issuing a contract with a professional service provider. Instead, the policy states that the Board may decide if soliciting RFPs is in the best interest of the District. Therefore, the District generally used past experience in selecting professionals rather than selecting professionals based on a competitive process. For example, the District has been using the same legal firm for over 10 years and the same physical therapist for over nine years without seeking competition. These professional service providers were paid $278,188 and $114,630, respectively, during the audit period.

During the fiscal year ended June 30, 2008, the District paid 48 professional service providers approximately $2 million. We reviewed payments that were made to eight professional service providers totaling $900,000 during the audit period and found that the services of all eight professional service providers were procured without soliciting RFPs or other competition. The professionals included two legal firms ($429,247), an individual hired to oversee a capital project ($178,424), an individual providing information technology (IT) consulting services ($89,000), an individual providing physical therapy services ($114,630), two financial advisors ($51,416) and an asbestos inspector ($37,111). The failure of District officials to solicit competition prior to procuring professional services increases the risk that services of the appropriate quality were not obtained at the lowest possible price.

Recommendation

5. The Board should revise its procurement policy to require District officials to solicit competition, prior to selecting and awarding contracts to professional service providers.

Information Technology

The use of IT affects the fundamental manner in which the District processes, records, and reports financial transactions. Therefore, the IT system and the data it holds are a valuable District resource. The District's widespread use of IT presents a number of internal control risks such as unauthorized access to data and the potential loss of data. Therefore, District officials must design an effective system of internal controls to safeguard computerized data from loss and misuse. This system should include policies and procedures to control and monitor access to financial data and a formal disaster recovery plan to minimize the damage that a disaster would cause to operations if the IT system fails.

The District uses financial software to process and maintain the District's financial transactions. District officials have not developed policies and procedures to protect critical financial data. User access rights are not properly established, remote access is not being monitored, audit trail logs are not being reviewed and the District does not have a formal disaster recovery plan. As a result, critical financial data is subject to an increased risk of loss or misuse.

User Access – To help ensure the proper segregation of duties and internal controls, a computer system should allow users to access only those functions that are necessary based on their job descriptions and responsibilities. User accounts provide a means to identify and differentiate users and, therefore, to control electronic access. Generally created by the system administrator, user accounts contain user-specific information such as passwords and access rights to files, applications, and other computer resources. District officials must ensure that user access rights are appropriate to employees' job descriptions and levels of responsibility and that those rights are promptly adjusted or deactivated when employees' responsibilities change or upon their separation from District service.

The District's financial software includes modules that segregate various financial recording and reporting processes. Available access privileges include the ability to add, update, delete, and print transactions within these modules. When such access is properly restricted according to users' job duties, a proper segregation of duties is maintained so that no individual user can control multiple aspects of a financial transaction.

District officials did not effectively safeguard the District's computerized financial data, and had no policies or procedures

detailing the authorization and documentation requirements for user account additions, deletions, or changes. We compared the assigned user access rights to the job descriptions of 14 employees who used the financial software and found that two of these employees, the principal account clerk and the Assistant Business Administrator, had access rights that were not in accordance with their job functions.

During our audit period, the Assistant Business Administrator had system administrator rights which included the ability to add, delete and modify user access rights and passwords, including his own, to the financial software. The Assistant Business Administrator was not authorized to perform this function and it is not compatible with his job description. In addition, the principal account clerk had rights to make budget transfers, prepare and void checks, and prepare and modify purchase orders, all of which are duties outside of her function in the Business Office. After we brought the matter to the attention of District officials in August 2008, the Assistant Business Administrator's system administrator rights were revoked. However, the District has not established policies and procedures to properly restrict user access to the District's computerized financial data. This can result in unauthorized access to sensitive information, manipulation of District records, and the loss or destruction of critical or confidential data.

Audit Logs – A well-designed IT system should be capable of generating an audit log that provides a means of determining, on a constant basis, who is accessing the system and what transactions are being processed. Audit logs maintain a record of activity that includes the identity of each person who has accessed the system, the time and date of the access, and what activity occurred. Ideally, a manager should review these logs on a routine basis to monitor the activity of users who access the District's applications and data.

Although the financial software has the ability to track system activity, District officials did not implement procedures to periodically produce and review relevant reports such as audit logs, and exception and change reports. Therefore, it would be difficult for the District to identify unauthorized users or unauthorized transactions, such as the unauthorized wire transfers. As a result, unauthorized activity went undetected and there continues to be an increased risk that unauthorized activity could go undetected.

Remote Access – Remote access is the ability to access the District's computer system from the internet or other external source. Remote access must be controlled, monitored, and tracked so that only authorized individuals are allowed to access the District's computer system. These individuals have the same access to the system as

if they were using a computer in a District facility. Policies and procedures should address how remote access is granted, who is given remote access, as well as how remote access will be monitored and controlled.

The District has not implemented policies or established procedures that address remote access issues. The Assistant Superintendent for Business is responsible for authorizing remote access but she does not keep track of who is granted access and was unable to provide us with a list of users that have been granted this privilege. In addition, no one in the District monitors the activity of individuals who have been granted remote access to the District's computer system. Although activity passing through the firewall is logged, these logs are not retained and they are not reviewed on a routine basis.

Internal controls are compromised when remote access is not monitored and controlled. Accordingly, there is an increased risk that financial data could be manipulated, and errors and irregularities could occur and go undetected. These internal control weaknesses could lead to the loss of important financial data and cause serious interruption to the District's operations.

Disaster Recovery Plan – A good internal control system also includes policies that require the adoption of a formal disaster recovery plan (DRP) to prevent loss of computer equipment and data, as well as procedures for recovery in the event of a loss. The DRP should identify precautions to be taken to minimize the effects of a disaster so that the organization will be able to either maintain or quickly resume mission-critical functions. It should also include a significant focus on disaster prevention. The DRP should be distributed to all responsible parties, periodically tested and updated as needed.

District officials have not established formal policies or procedures to address potential disasters. In the event of a disaster, District personnel have no guidelines or plan to follow to prevent the loss of equipment and data or to initiate data recovery procedures. As a result of these internal control weaknesses, the District risks losing computer-processed financial and non-financial data with no means to ensure its recovery, in order to facilitate the continuance of normal operations.

Recommendations

6. District officials should review and revise user access rights to the financial software to ensure that users have access only to those functions needed for their job responsibilities.

7. District officials should develop policies and procedures requiring that all user account additions, deletions, and changes are properly

authorized and documented. These procedures should include steps for the periodic review of user access rights and their modification or deactivation, as appropriate, when employees' job responsibilities change or employees leave District service.

8. District officials should implement procedures to have audit logs periodically reviewed.

9. The Board and District officials should adopt policies and establish written procedures to control and monitor remote access to financial computer data.

10. District officials should develop a formal disaster recovery plan.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

The District officials' response to this audit can be found on the following pages.

LINDENHURST PUBLIC SCHOOLS

Administration Building 350 Daniel Street Lindenhurst, NY 11757

Tel: 631-867-3001 Fax: 631-867-3008 rnathan@lindenhurstschools.org

Richard Nathan

Superintendent of Schools

January 26, 2010

Mr. Jeffrey Leonard
State Of New York
Office of the Comptroller
New York State Office Building
250 Veterans Memorial Highway, Room 3A10
Hauppauge, New York 11788

Dear Mr. Leonard:

Thank you for the opportunity to respond to your recent review of the Lindenhurst UFSD. We welcome the additional oversight and recommendations for further improving the operations and internal control environment of our District.

The auditors were physically present in the Lindenhurst UFSD from July 2008 to December 2008. The audit covered the period from July 1, 2007 to June 30, 2008. We have reviewed the draft report and are providing the following information in response to issues and recommendations raised in the reports.

Business Office – Electronic Wire Transfer

We acknowledge that our controls had weaknesses that were exploited by an outside criminal enterprise. These controls have now been significantly improved. The District only has the ability to process online wire transfers with two banks. Dual authorization has been in force for all online wire transfers since July 2007, immediately following the incident, to ensure the district could not fall victim to this type of criminal activity again. Wire transfers in the other three institutions were only processed via phone calls or by fax (no internet transfers). The wires were verified by a return call to the district before the transfer was completed. Of the three banking institutions where internet transfers were not used, the district had access to make only internal transfers (no external transfers were made) in one of the institutions. Currently, dual authorization is in place for **all** banking institutions regardless of the type of transfer taking place. Procedures for wire transfers are written and included in the business office manual produced in January, 2009.

See Note 1 Page 29

We have spoken to prior administration officials who were in positions of authority at the time this matter transpired. These administrators told us that the bank officials indicated to District administration that the bank would be contacting the FBI, who would be doing a thorough investigation. The FBI did, in fact, investigate the theft. This was recently corroborated by a detective from the Suffolk County District Attorney's office who investigated the incident.

See Note 2 Page 29

The bank recovered $496,590. The District received $102,487 from its insurance company and the bank reimbursed the district for the $2500 deductible. Therefore, the entire $601,577 was restored to the district accounts and there was no loss to the District.

The former superintendent has indicated to us that after the money was fully recovered/restored, he shared that information with the community at a Board of Education meeting as part of his superintendent's report.

Claims Processing

The district issued a RFP for a Claims Auditor in October, 2008. The claims auditor's responsibility is to ensure that all payments are appropriate and necessary. The new claims auditor began working in Lindenhurst during January 2009 and reviews **all** claims prior to the release of checks.

In reference to the following comment:

"An office supply store was paid $1000, for 10 $100 gift certificates on November 19, 2007." "Although the purchase order for the expenditure stated that the Board approved these gift certificates, we found that the purchase was not approved by the Board."

The certificates were given to teachers to buy supplies for special projects. This purchase was under the auspices of the OWL Teacher Center Program using their teacher center grant. In the future, all purchases will be reimbursed upon the submission of an invoice or bill from the vendor showing the items purchased. This purchase was approved by the policy board of the OWL Teacher Center, not the Board of Education.

See Note 3 Page 29

Professional Services

General Municipal Law does not require solicitation of RFP's for professional services. The District operated in a manner consistent with Board policy as well as state laws and regulations. The Board of Education policy does not require RFP's for all services. For example, for students receiving physical therapy we believe it is not educationally sound to shuttle students back and forth between different providers simply because one provider might have bid one dollar lower than a competitor. Also, using different attorneys from year to year might make long term and continuing litigation difficult.

See Note 4 Page 29

Information Technology

Remote access is monitored and controlled by the Director of Technology. The Director of Technology knows exactly who has remote access and could have easily provided a list to the auditors had he been asked. During the time period reviewed, remote access was only granted to the Assistant Superintendent of Business and approved by the Superintendent. User agreements were developed and all current users have signed them along with the Assistant Superintendent of Business. These forms are currently kept on file with the Director of Technology.

Changes and/or additions to security in the financial software must be requested in writing and approved by the Assistant Superintendent for Business prior to any changes being instituted by the information technology department. This procedure was put into place on August 6, 2008. Policies and procedures were written in January of 2009.

RECOMMENDATIONS.

1. The Board and District officials should investigate all thefts of District funds and the appropriate authorities should be notified.

Response:

The bank informed the district that the FBI was notified and that a full investigation was underway. Administrators who were in place at the time of this incident told us that they felt appropriate legal authorities were informed by the bank. However, in the future, an incident such as this will include the notification of all appropriate local legal authorities by the district to ensure a full investigation occurs.

See Note 2 Page 29

2. The Board should adopt, and employees should adhere to, written policies for cash receipts and disbursements. These policies and procedures should include the following requirements:

> **Wire transfers should be reviewed and approved by someone other than the individual who initiated the transfer. This second individual should also receive the transfer confirmation from the bank.**

Response:

Security was changed in July 2007 so that all external internet wire transfers required dual authorization. Currently, all external wire transfers regardless of the process used require dual authorization.

See Note 1 Page 29

> **Cash receipt procedures should be adequately segregated. The duties of opening the mail should be segregated from the duties of handling cash. In addition, the duties of recording cash receipts should be segregated from the duties of preparing and depositing cash.**

Response:

In September 2008 the procedures for handling cash receipts were segregated out among three separate employees in the business office. An account clerk is responsible for logging in all cash as it is received and issuing receipts. The principal account clerk is responsible for making the bank deposits and recording the monies in the financial software package. The treasurer is responsible for verifying all monies received by the account clerk are deposited into our bank account and recorded in the financial software by our Principal Account Clerk. This new procedure was implemented during the period the auditors were on site and shared with the auditing team.

> **The Treasurer should keep personal control and custody of her signature disk and directly oversee its use. Access to her signature disk should not be available to unauthorized individuals.**

Response:

In August 2008 the District advertised for a full time treasurer. The treasurer began in October 2008. The treasurer is the only person with access to the signature disk. Additionally, security was changed so that the only person with the ability to print checks through the financial software and check printing software is the treasurer. This new procedure was implemented during the period the auditors were on site and shared with the auditing team.

3. The Board should ensure that the claims auditor conducts a proper audit of all District claims in accordance with laws, regulations, and District policies.

Response:

The District advertised a RFP for the internal claims auditor on September 20, 2008. The internal claims auditor was appointed on January 7, 2009. **All** checks issued for **all** funds since January 1, 2009 have been reviewed prior to disbursement.

4. The Board and District officials should ensure that claims are paid only after a thorough audit by the claims auditor.

Response:
Effective January 1, 2009, **all** invoice packets are thoroughly reviewed by the claims auditor prior to disbursement.

5. The Board should revise its procurement policy to require District officials to solicit competition, prior to selecting and awarding contracts to professional service providers.

Response:

General Municipal Law does not require solicitation of RFP's for professional services. The District operated in a manner consistent with Board policy as well as state laws and regulations. The Board policy does not require RFP's for all services. The District has increased its use of RFP's for professional services and will continue to increase its use of RFP's for professional services in the future.

6. District officials should review and revise user access rights to the financial software to ensure that users have access only to those functions needed for their job responsibilities.

Response:

A review of all user security by the Assistant Superintendent of Business began in August 2008 and is a continuing process. Written memos by the Assistant Superintendent of Business outlining all changes are kept on file with the Director of Technology.

7. District officials should develop policies and procedures requiring that all user account additions, deletions and changes are properly authorized and documented. These procedures should include steps for the periodic review of user access rights and their modification or deactivation, as appropriate, when employees' job responsibilities change or employees leave the District service.

Response:

Changes and/or additions to security in the financial software must have written approval from the Assistant Superintendent for Business prior to any changes being made and/or additions being implemented by the information technology department. This procedure was put into place on August 6, 2008. Memos are kept on file in the technology department. This new procedure was implemented during the period the auditors were on site and shared with the auditing team.

8. District officials should implement procedures to have audit logs periodically reviewed.

Response:

Procedures have been implemented to produce audit logs periodically from our financial software. The District has arranged to have training on various audit logs by our financial software provider so that we can determine the best way to implement procedures to review the critical areas.

9. The Board and District officials should adopt policies and establish written procedures to control and monitor remote access to financial computer data.

Response:

The Director of Technology knows exactly who has remote access and could have easily provided that to the auditors. During the time period reviewed, remote access was granted to the Assistant Superintendent of Business and no other employees. This was approved by the Superintendent of Schools. A Remote Access Agreement form and procedures were developed and put into place effective December 2008. All new and previous users that have remote access have signed this agreement. This form must be approved by the Assistant Superintendent of Business before implementation and kept on file by the Director of Technology.

10. District officials should develop a formal disaster recovery plan.

Response:

The information technology department issued a memo to the superintendent and the Board of Education on September 30, 2009 and a follow up memo on October 13, 2009 outlining the importance of implementing a formal disaster recovery plan. On November 4, 2009, the technology department met with the Board of Education and District Administration to go over the particulars of instituting the disaster recovery plan. A detailed cost analysis has been provided to the Board of Education for the

implementation of this plan. On January 13, 2010, the Board of Education authorized a disaster recovery plan which fixes current technical limitations and provides the platform needed to virtualize critical servers as well as creates an off-site center for both our financial software and the business share. The plan also provides the space necessary for future data growth.

We trust that these responses provide assurance that we take your comments seriously and are prepared to further improve the operations and internal control environment to ensure the continued integrity of our operations.

Sincerely yours,

Richard Nathan
Superintendent of Schools

RN/tp

APPENDIX B

OSC COMMENTS ON THE DISTRICT'S RESPONSE

Note 1

In July 2008, District officials informed us that in July 2007, six unauthorized on-line wire transfers amounting to $601,577 were initiated that improperly transmitted money from a general fund bank account to various non-District accounts in other banks. We asked District officials to provide us with the policies and written procedures governing the wire transfer process. Over a year after the thefts occurred, the District still had no policies or written procedures over the wire transfer process. We asked the principal account clerk, in charge of initiating all of the District's wire transfers, to transcribe the procedures used to process wire transfers. The District processed internal and external wire transfers from accounts kept at six banks. Two banks processed wire transfers on-line, three banks processed wire transfers using a fax request and one bank initiated wire transfers only after a telephone request. As of August 2007, dual authorization was being used to process on-line wire transfers only. There was no second authorization needed to process fax requests and the one bank which processed wire transfers by phone did call the District back for verification but they were not required to call a person other than the person initiating the transfer.

Note 2

The Board and District officials should have informed appropriate law enforcement officials as soon as the thefts occurred. During our fieldwork, District officials could not confirm whether the bank had ever contacted the FBI. In addition, District employees stated that they were never contacted or questioned by law enforcement officials about the incident. District officials gave us a copy of a letter from the Bank dated January 28, 2008. This letter stated that the Bank completed their investigation and they concluded that they (the Bank) were not responsible for the loss. The letter also stated that the theft was initiated by access information (Password) provided by the District. The letter did not indicate that law enforcement authorities were contacted. The Suffolk County District Attorney's office, more than two years later, confirmed that the FBI was involved in an investigation of the thefts.
.

Note 3

The policy board of the OWL Teacher Center had no authority to approve these purchases for payment. The Board of Education chose to delegate their responsibility for auditing claims and established the position of a claims auditor. Therefore, the claims auditor was the only individual authorized to approve this claim for payment.

Note 4

The District's purchasing policy does not require officials to solicit competitive proposals prior to issuing a contract with a professional service provider but the solicitation of competition prior to procuring professional services would help ensure that these types of services are obtained at the lowest possible price.

APPENDIX C

AUDIT METHODOLOGY AND STANDARDS

Our overall goal was to assess the adequacy of the internal controls put in place by officials to safeguard District assets. To accomplish this, we performed an initial assessment of the internal controls so that we could design our audit to focus on those areas most at risk. Our initial assessment included evaluations of the following areas: financial oversight, cash receipts and disbursements, purchasing, payroll and personal services and information technology.

During the initial assessment, we interviewed appropriate District officials, performed limited tests of transactions and reviewed pertinent documents, such as District policies and procedures manuals, Board minutes, and financial records and reports. In addition, we obtained information directly from the computerized financial databases and then analyzed it electronically using computer-assisted techniques. This approach provided us with additional information about the District's financial transactions as recorded in its databases. Further, we reviewed the District's internal controls and procedures over the computerized financial databases to help ensure that the information produced by such systems was reliable.

After reviewing the information gathered during our initial assessment, we determined where weaknesses existed, and evaluated those weaknesses for the risk of potential fraud, theft and/or professional misconduct. We then decided on the reported objective and scope by selecting for audit those areas most at risk. We selected Business Office operations, claims processing, purchasing and information technology for further audit testing.

Our audit procedures included the following:

- We reviewed the minutes of the Board meetings and the Board policy manual.
- We interviewed appropriate District officials in order to obtain an understanding of the organization, the District's accounting system, and to identify key personnel.
- We tested selected records and transactions, performed analytical procedures, and examined pertinent documents for the period July 1, 2007, through June 30, 2008.
- We observed operations and examined records to verify that receipts, disbursements, investments and electronic wire transfers were made by authorized personnel.
- We verified that daily cash receipts, investment instruments, blank checks, bank records, and signature plates were physically secured.
- We examined claims for evidence of audit and approval, including post audit of claims paid prior to audit.
- We reviewed the formal policy for purchasing and determined if it adequately addresses the procurement of goods and services.

- We determined if the District issued RFPs before entering into contracts for professional services.

- We reviewed all computer use and IT policies.

- We interviewed the Director of Technology and other District officials regarding computer use policies and procedures.

- We examined user permission reports to determine if access rights to the computer systems were granted using the concept of least privilege.

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.

APPENDIX D

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 E

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

Steven J. Hancox, Deputy Comptroller
John C. Traylor, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BUFFALO REGIONAL OFFICE
Robert Meller, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
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

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
Eugene A. Camp, 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

BINGHAMTON REGIONAL OFFICE
Patrick Carbone, Chief Examiner
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

GLENS FALLS REGIONAL OFFICE
Karl Smoczynski, Chief Examiner
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

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

HAUPPAUGE REGIONAL OFFICE
Jeffrey P. Leonard, 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