



Oysterponds Union Free School District

Internal Controls Over Selected Financial Operations

Report of Examination

Period Covered:

July 1, 2005 — April 30, 2007

2008M-145



Thomas P. DiNapoli

Table of Contents

	Page
AUTHORITY LETTER	2
EXECUTIVE SUMMARY	3
INTRODUCTION	5
Background	5
Objective	5
Scope and Methodology	5
Comments of District Officials and Corrective Action	5
TREASURER'S OPERATIONS	7
Authorized Signatures	7
Segregation of Duties	7
Recommendations	8
INFORMATION TECHNOLOGY	9
Policies and Procedures	9
Audit Logs	11
Recommendations	11
APPENDIX A Response From District Officials	13
APPENDIX B Audit Methodology and Standards	19
APPENDIX C How to Obtain Additional Copies of the Report	20
APPENDIX D Local Regional Office Listing	21

State of New York Office of the State Comptroller

Division of Local Government and School Accountability

October 2008

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 is mandated to oversee 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 Oysterponds 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 Oysterponds Union Free School District (District) is governed by the Board of Education (Board) which comprises seven 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 is one school in operation within the District which houses Kindergarten through Grade 6. The District employs approximately 30 employees and has an enrollment of approximately 110 students in grades K-6. An additional 100 students attend grades 7-12 at a neighboring school district. The District's budgeted expenditures for the 2006-07 fiscal year were \$5,231,707, which were funded primarily with real property taxes, State aid and grants.

Scope and Objective

The objective of our audit was to examine the District's internal controls over selected financial operations for the period July 1, 2005 through April 30, 2007. Our audit addressed the following related questions:

- Has the District established adequate internal controls over the Treasurer's duties and are those controls operating effectively?
- Are internal controls over the information technology systems appropriately designed to protect electronic hardware and data?

Audit Results

Internal controls over the District Treasurer's duties were not appropriately designed and operating effectively. Although Education Law precludes a member of the Board from assuming the duties of the Treasurer, we found that the Board inappropriately appointed one of its members to act as Assistant Treasurer. District officials also failed to segregate the Treasurer's cash receipts and disbursement duties, which included receiving cash, preparing and making bank deposits, signing checks, making wire transfers, transferring cash between funds, and reconciling the bank accounts. Although our testing revealed no discrepancies, with these internal control weaknesses, the risk is increased that errors or irregularities could occur and not be detected or corrected.

Internal controls over the information technology system were not appropriately designed to protect electronic hardware and data. There were no policies and procedures for users' computer access

rights. Proper access controls are essential to identify and differentiate among users. Lack of controls over access could lead to the loss or misuse of critical financial data. District officials have not established adequate policies and procedures over the physical security of its information technology (IT) assets. The lack of adequate policies and procedures may be disruptive to District services, and costly equipment could be damaged, destroyed or stolen. Due to a lack of formal backup and disaster recovery policies and procedures, the malfunction of the District's backup system remained undetected for an undeterminable amount of time. Had the District experienced disaster or a computer failure, the District could have lost important financial data and experienced serious interruptions of critical business operations. Finally, District officials failed to review audit logs that were generated by the District's computerized financial system. Without regular review of audit logs, errors could occur and not be detected or corrected in a timely manner.

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 they planned to initiate corrective action.

Introduction

Background

The Oysterponds Union Free School District (District) is located in the Town of Southold, Suffolk County. The District is governed by the Board of Education (Board) which comprises seven 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 is one school in operation within the District which houses Kindergarten through Grade 6. The District employs approximately 30 employees and has an enrollment of approximately 110 students in grades K-6. An additional 100 students attend grades 7-12 at a neighboring school district. The Treasurer and District Clerk manage the District's Business Office, and process financial transactions using a computerized financial management system. The District's budgeted expenditures for the 2006-07 fiscal year were \$5,231,707, funded primarily with State aid, real property taxes, and grants.

Objective

The objective of our audit was to examine the District's internal controls over selected financial operations. Our audit addressed the following related questions:

- Has the District established adequate internal controls over the Treasurer's duties and are those controls operating effectively?
- Are internal controls over Information Technology systems appropriately designed to protect electronic hardware and data?

Scope and Methodology

We examined the internal controls over selected financial operations of the District for the period July 1, 2005 to April 30, 2007.

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 B 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 they planned to initiate corrective action.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of the GML, 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 forwarded to our office within 90 days. 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.

Treasurer's Operations

It is essential that District officials establish adequate controls over cash receipts and disbursements, including requiring that key duties be segregated so that no one employee controls all steps of a transaction. When internal controls are not designed appropriately or operating effectively, the risk is increased that errors or irregularities may occur and not be detected and corrected.

We found that internal controls over the Treasurer's operations need to be improved. The Board improperly appointed one of its members as Assistant Treasurer. In addition, District officials did not properly segregate the Treasurer's cash receipts and disbursements duties. Although our testing revealed no discrepancies, these internal control weaknesses could lead to errors or irregular activities occurring and not being detected.

Authorized Signatures

The Board appointed the Treasurer as the custodian of all District moneys. Therefore, the Treasurer is authorized to sign all checks issued on behalf of the District. Education Law prohibits Board members from holding the office of Treasurer. However, the Board may, in its discretion, require another District officer to countersign District checks. In addition, the Board may, by resolution, designate one of its members to sign checks in the absence of either the Treasurer or the District officer who is authorized to countersign District checks.

At the July 12, 2006 organizational meeting, in addition to appointing the Treasurer, the Board appointed a Board member as an Assistant Treasurer. Both the Treasurer and the Assistant Treasurer were authorized to sign as the sole signatory on all checks under \$5,000, and both of their signatures were required on checks \$5,000 and above. By authorizing one of its members to sign checks under \$5,000 as a sole signatory, the Board allowed one of its members to also act as Treasurer, which is prohibited by Education Law. Although our tests of the 516 checks issued during our audit period found that the Board member did not sign any checks that required only one signature, the appointment of a Board member as Assistant Treasurer is not appropriate.

Segregation of Duties

An important component of any internal control system is proper segregation of duties over cash receipts and disbursements, which ensures that no one person controls all phases of a transaction. Concentrating key duties (such as authorization, recordkeeping and custody) with one individual with little or no oversight weakens internal controls and significantly increases the risk that errors and/or

irregularities might occur and go undetected. If complete segregation of duties is not practicable, management oversight can mitigate this internal control risk and help ensure that errors are detected and corrected in a timely manner.

District officials did not effectively segregate the Treasurer's cash receipts and disbursement duties or establish sufficient compensating controls to mitigate the potential risk. The Treasurer maintained the District's general journals, cash receipts and disbursement records, and general and subsidiary ledgers. He also received cash; prepared bank deposit tickets; made bank deposits; signed checks; performed, recorded and approved wire transfers; transferred cash between funds; and reconciled bank accounts. When performed by one person, these duties are incompatible because the Treasurer could make improper transfers and payments and then conceal these activities by creating misleading accounting entries.

Due to the increased risk associated with the lack of segregation of duties over cash transactions, we reviewed all six bank and wire transfers reported for October 2006 totaling \$610,427 that were completed by the Treasurer and were not approved or reviewed by another individual. Our review of the six transactions disclosed no errors or irregularities. However, District management's failure to properly segregate the Treasurer's duties or provide a compensating control, such as enhanced management review, can result in errors or irregularities occurring and not being detected and corrected in a timely manner.

Recommendations

1. The Board should not designate any Board member as Assistant Treasurer.
2. The Board should ensure that the official depositories are notified of any eventual changes of signatories to the District's bank accounts.
3. District officials should ensure that functions related to cash receipts and disbursements, including wire and bank transfers, are properly segregated.

Information Technology

Computer data is a valuable and essential resource. District officials rely upon computer data for making financial decisions and for reporting to State and Federal agencies. If the computers on which this data is stored fail, or the data is lost or altered, the results could range from inconvenient to catastrophic. Even small disruptions in electronic data systems can require extensive effort to evaluate and repair. For this reason, District officials need to control and monitor access to computer data systems. District officials also need to make sure that computerized data is physically secure and must implement a formal disaster plan to provide guidance on preventing the loss of, as well as the recovery of, computer data in the event of a disaster. In addition, the periodic review of computer-generated reports, such as audit logs, can help District officials monitor employees' work on the computerized accounting system.

District officials have not established adequate internal controls over computer operations to insure that its computerized data is safeguarded. Specifically, officials have not adopted formal policies for access rights and the physical security of computer equipment and data. Also, due to lack of formal policies and procedures, the District's computer equipment and data are not adequately protected and backed up and there is no formal disaster recovery plan. In addition, District officials failed to review the audit logs that were generated by the computerized financial system. As a result of these weaknesses, there is an increased risk that unauthorized users can access and compromise the District's computer system and data, and District employees have no guidance on what steps they should take to recover computerized assets in the event of a disaster. Without the periodic review of audit logs, financial errors could occur and not be detected in a timely manner.

Policies and Procedures

Access Rights — It is important that an internal control system include policies and procedures to ensure that only authorized users have active user accounts, and that user accounts are deactivated as soon as employees leave District service. User accounts identify the specific users of a particular network, computer and/or application. These accounts contain information such as passwords and the access rights to files, applications, directories and other computer resources. The System Administrator should only create user accounts based upon management's written authority.

The District did not establish policies or procedures detailing the authorization and documentation requirements for the additions,

deletions or changes of user accounts for District employees or students. Without such documentation, the District is unable to determine who authorized access for specific user accounts, when access was granted or revoked, and the extent of the access that was permitted.

Because of the lack of formal policies governing access rights, the risk that unauthorized users could gain access to a system and change, destroy or manipulate computer data is greatly increased. Further, if a problem did arise, it would be very difficult for District officials to determine who authorized access, when access was given or revoked, and the type of access that was granted.

Physical Security — Another key component of an internal control structure is the institution of policies and procedures relating to physical security over IT assets (i.e., computer hardware, servers and wiring closets). These policies and procedures must ensure that the computer assets are protected by limiting access to those assets and securing assets from fire and water damage. Securing computer hardware, servers and patch panels¹ is an important first step to physically securing IT assets.

District officials have not established adequate policies and procedures to physically secure IT assets, which resulted in various security deficiencies. The District maintains its financial data on one server and student data on another. Both of the District's servers are located in an unlocked metal closet in one of the District's offices. The door to the office can be accessed by anyone with a master key, including the Principal and two custodians.

Without physical security, all other security measures may be ineffective. Physical threats, whether internal or external, malicious or inadvertent, could lead to damaged or stolen hardware and/or the release of personal or other confidential information. Security breaches can result in monetary loss and the need for extensive effort to correct.

Data Backup — Data must be backed up (i.e., copy made) on a routine basis, and it is important that the backup copy be stored at an environmentally and physically secure off-site location. The District has not established formal policies and procedures for backing up District data, including financial data.

¹ A device that filters and forwards information between components in the network

The District was utilizing a tape drive to back up its server daily. However, in the spring of 2007, District officials realized that the backup system was not working properly and could not determine how long the system had been malfunctioning. Additionally, a copy of the backup tape was not stored in a secure off-site location. Due to the lack of formal backup policies and procedures, the failure of the District's backup system remained undetected for an undeterminable period of time. During that time, the District was at an increased risk of losing most, if not all, of their computer-processed data. Had there been an unforeseen event, such as computer hardware failure, fire or water damage, District officials would have had no means to ensure data recovery to allow them to continue normal operations in a timely manner.

Disaster Recovery — A strong system of internal controls includes a Disaster Recovery Plan (DRP) to help prevent the loss of computer equipment and data. A DRP must include procedures for recovery in the event of an actual loss and the precautions to be taken to minimize the effects of a disaster so that District officials can either maintain or quickly resume mission-critical functions. The plan may also include a significant focus on disaster prevention.

District officials have not developed a DRP. As a result, the District may, in case of a disaster or unforeseen event, experience the loss of important financial data and serious interruptions to District operations, such as staff not being able to process checks to pay vendors and employees.

Audit Logs

Computer-generated monitoring reports can be used to help offset control weaknesses resulting from the lack of segregation of duties. One such report is an audit log, which is a record of all changes a user performs within the software, the location of the computer from which the user made changes, and the times and dates the user made the changes. The District's financial software program has an audit log in place. If District officials periodically reviewed these audit logs, they could track the activities of each user within the system and ensure that users are not performing any duties that are not part of their job descriptions. However, District officials do not review the software program's audit logs. Unless District officials provide for an independent review of the financial system's audit logs, they may not detect and correct errors or irregularities that may occur in a timely manner.

Recommendations

4. District officials should develop and monitor compliance with formal policies and procedures relating to access rights, physical security and data backup.

5. District officials should perform daily backups of the network, store backups in a secure location, and store backup copies in a physically secure off-site location.
6. District officials should develop a disaster recovery plan to help prevent the loss of computer equipment and data.
7. District officials should regularly review audit logs that are generated by the computerized financial system.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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



OYSTERPONDS U.F.S.D. IN ORIENT
23405 MAIN ROAD
ORIENT NY 11957

Telephone 631 323-2410
Fax 631 323-3713
Website: www.oysterponds.org

Dr. Stuart Rachlin
Superintendent

September 19, 2008

Hauppauge Regional Office
Office of the State Comptroller
NYS Office Building, Room 3A10
Veterans Memorial Highway
Hauppauge, NY 11788-5533

Dear Sirs,

The Board of Education and the administration of the Oysterponds UFSD in Orient are grateful to the representatives of the Hauppauge Regional Office for the time and effort they have expended to create the *Report of Examination #2008M-145* covering internal controls over selected financial operations. As a school district of approximately 105 students in grades K-6 (with another 100 students tuitioned to Greenport UFSD in grades 7-12), we recognize that our size requires developing innovative ways and our processes need to be refined to ensure maximum control over our finances. We agree that all recommendations provide opportunities for improvement. Please accept this letter as a response and a Corrective Action Plan, representing both the Board of Education and the administration of this district.

Unit Name: Oysterponds Union Free School District
Audit Report Title: Internal Controls over Selected Financial Operations
Audit Report Number: 2008M-145

1. Audit Recommendation

The Board should not designate any Board member as Assistant Treasurer.

Implementation Plan of Action

By Board of Education motion, the title "Assistant Treasurer" assigned to the Board of Education president shall be changed to "Co-signer". The role of "Deputy Treasurer" shall, similarly, be established through Board of Education motion and will be assigned to a non-Board of Education member (presently, the Director of Special Education); this person shall be permitted to sign checks in the absence of the Treasurer.

Implementation Date

September 10, 2008

Person Responsible for Implementation

Board of Education

2. Audit Recommendation

The Board of Education should ensure that the official depositories are notified of any eventual changes of signatories to the District's bank accounts.

Implementation Plan of Action

The Treasurer* of the Oysterponds UFSD in Orient shall obtain a listing of all accounts and their signatories and, subsequent to any change made thereafter by virtue of Board of Education motion, shall notify our depositories of any eventual changes of signatories. The District Clerk shall request evidence of such notification.

Implementation Date

Immediately

Person Responsible for Implementation

Superintendent and District Clerk

3. Audit Recommendation

District officials should ensure that functions related to cash receipts and disbursements, including wire and bank transfers, are properly segregated.

Implementation Plan of Action

We now have:

- One employee receiving cash and checks and entering same into Cash Receipts Record Book
- District Clerk creating deposit slip and depositing same
- Treasurer comparing receipted slip with Cash Receipts Log

Incoming wire transfers shall be treated in the same way.

The District follows the process listed below with regard to disbursement of checks:

- The Superintendent of Schools, who also acts as Purchasing Agent, compares invoice to purchase order and approves for payment.
- District Clerk generates check.
- District Clerk prepares the warrant for BOE approval.
- The Treasurer* ensures that there are sufficient funds on deposit to satisfy the obligation and signs checks thereafter. With regard to checks in excess of \$5,000, an additional signatory is required as authorized by the Board of Education at its Reorganizational Meeting (as addressed in Audit Recommendation #1).
- The Board of Education, individually and as a group, reviews each check for accuracy and initials/dates each invoice to indicate agreement.
- The Board of Education approves the warrant at a Regular Meeting.
- A district employee with no disbursement responsibilities folds and prepares checks for mailing.

As for wire transfers involving solely School District bank accounts, the Treasurer shall write up the transfer, and the Superintendent shall OK the transfer; we will ask our depository to notify the Superintendent in writing that a transfer has been implemented. The Superintendent shall compare the bank notice with the original transfer request. We shall also provide written orders to our depository in which we specify transfer rights (times of day, days of the week, authorized users, limitations of accounts between which transfers may occur) and a listing of permitted payees with top allowed dollar limits.

Implementation Date

October 1, 2008

Person Responsible for Implementation

Superintendent of Schools

4. Audit Recommendation

District officials should develop and monitor compliance with formal policies and procedures relating to access rights, physical security and backup.

Implementation Plan of Action

1. The District shall develop, and the BOE shall adopt, procedures governing access rights, physical security and backup.
2. The rack in which the server resides shall be locked at all times, with access to the key provided to our Technology teacher and, on an as-needed basis, to our LAN support consultants.
3. The Building & Grounds Committee shall review the security of the servers, routers and switches and the physical plant thereof and shall make a recommendation to the Superintendent no later than December 31, 2008 on how to secure that area.

Implementation Date

December 31, 2008

Person Responsible for Implementation

Superintendent of Schools
BOE Buildings & Grounds Committee

5. Audit Recommendation

District officials should perform daily backups of the network, store backups in a secure location, and store backup copies in a physically secure off-site location.

Implementation Plan of Action

The Technology teacher shall initiate the daily back-up of the network and make a copy of that back-up; the District Clerk shall lock the back-up tape in a cabinet in his/her office. A copy of the back-up shall be brought off-site by the Superintendent on a weekly basis and stored at his/her home.

Implementation Date

September 16, 2008

Person Responsible for Implementation

Technology teacher, District Clerk, Superintendent of Schools

6. Audit Recommendation

District officials should develop a disaster recovery plan to help prevent the loss of computer equipment and data.

Implementation Plan of Action

The Superintendent of Schools shall solicit similar plans from the local BOCES and regional school districts as well as from the district's external auditors and create a disaster recovery plan adapted to the Oysterponds UFSD.

Implementation Date

December 31, 2008

Person Responsible for Implementation

Superintendent of Schools

7. Audit Recommendation

District officials should regularly review audit logs that are generated by the computerized financial system.

Implementation Plan of Action

The Superintendent of Schools shall direct the District Clerk, effective immediately, to generate an audit log of [REDACTED] access on a monthly basis and to provide the Superintendent with this log; the Superintendent shall review the log to ensure that only appropriate access (days, time of day, type of access, modules accessed, persons who have accessed the system) was made to the program and shall initial the log with the date of said review. These logs shall reside in the District Clerk's office through the period of an end-of-year audit by the school's external auditors.

Person(s) Responsible for Implementation

Superintendent of Schools
District Clerk

Implementation Date

October 1, 2008

* We are presently in transition between Treasurers but are ensuring appropriate segregation of duties.



(Dr.) Stuart Rachlin, Superintendent



Edward W. Webb – President,
Board of Education

cc: New York State Commissioner of Education Richard Mills

APPENDIX B

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: cash receipts and disbursements, purchasing, payroll and personal services, and capital assets and consumable inventories.

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 upon the reported objectives and scope by selecting for audit those areas most at risk. We selected the Treasurer's operations and information technology for further audit testing.

- We interviewed District officials and employees to learn about existing internal control systems.
- We interviewed Board members about the claims process, including authorized signatures.
- We tested bank and wire transfers that were completed by the Treasurer to determine their accuracy and whether they were made for appropriate District purposes.
- We reviewed the District's computer access and security protocols and procedures.
- We reviewed who had remote access and determined how the District monitored or tracked the remote access activity.
- We reviewed the District's financial system to determine whether it was capable of generating audit logs, and whether District officials reviewed these audit logs.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). Such standards require that we plan and conduct our audit to adequately assess those District operations within our audit scope. Further, those standards require that we understand the District's management controls and those laws, rules and regulations that are relevant to the District's operations included in our scope. An audit includes examining, on a test basis, evidence supporting transactions recorded in accounting and operating records and applying such other auditing procedures as we consider necessary in the circumstances. We believe that our audit provides a reasonable basis for the findings, conclusions, and recommendations contained in this report.

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
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