



# Ausable Valley Central School District Internal Controls Over Selected Financial Activities

## Report of Examination

Period Covered:

July 1, 2005 — June 30, 2007

2007M-257



Thomas P. DiNapoli

# Table of Contents

	<b>Page</b>
<b>AUTHORITY LETTER</b>	3
<b>INTRODUCTION</b>	5
Background	5
Objective	5
Scope and Methodology	5
Comments of District Officials and Corrective Action	6
<b>EXTRA-CLASSROOM ACTIVITY FUNDS</b>	7
Recommendations	8
<b>INFORMATION TECHNOLOGY</b>	10
Computer System Access	10
Audit Logs	13
Physical Security Over Network Servers and Component Parts	13
Data Backup	14
Disaster Recovery	14
Recommendations	14
<b>APPENDIX A</b> Response From District Officials	16
<b>APPENDIX B</b> Audit Methodology and Standards	19
<b>APPENDIX C</b> How to Obtain Additional Copies of the Report	21
<b>APPENDIX D</b> Local Regional Office Listing	22

# State of New York Office of the State Comptroller

---

---

## **Division of Local Government and School Accountability**

December 2007

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 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 Ausable Valley Central School District, entitled Internal Controls Over Selected Financial Activities. This audit was conducted pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution, and 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*

# Introduction

## Background

The Ausable Valley Central School District (District) is located in the Towns of Ausable, Black Brook, and Peru in Clinton County, the Towns of Chesterfield, Jay, Keene, Willsboro, and Wilmington in Essex County, and the Town of Franklin in Franklin 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. Responsibilities relating to District finances, accounting records and reports are largely those of the School Business Executive.

There are three schools in operation within the District, with approximately 1,280 students and 280 employees. The District's budgeted expenditures for the 2006-07 fiscal year were \$22.6 million, which were funded primarily with State aid, real property taxes, and grants.

The District reported approximately \$22.5 million in general fund expenditures during the 2006-07 fiscal year. During the same year, the extra-classroom activity fund recorded more than \$238,500 in receipts and disbursements. The District has approximately 700 individual computers that are networked together. District employees use computers in day-to-day operations for instructional purposes and to process financial transactions.

## Objective

The objective of our audit was to determine if the District had established effective internal controls over extra-classroom activity funds and information technology. Our audit addressed the following related questions:

- Are internal controls over extra-classroom activity funds adequate?
- Are internal controls over the District's information technology system appropriately designed to protect electronic data?

## Scope and Methodology

During this audit we examined the District's control environment and its internal controls, specifically related to extra-classroom activity funds and information technology, for the period July 1, 2005 to June 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 General Municipal Law, Section 2116-a (3)(c) of the Education Law and Section 170.12 of the Regulations of the Commissioner of Education, the Board must approve a corrective action plan that addresses the findings in this report, forward the plan to our office within 90 days, forward a copy of the plan to the Commissioner of Education, and make the plan available for public review in the District Clerk's office. For guidance in preparing the plan of action, the Board should refer to applicable sections in the publication issued by the Office of the State Comptroller entitled *Local Government Management Guide*.

## Extra-Classroom Activity Funds

The Regulations of the Commissioner of Education (Regulations) require each school district's board of education to make rules and regulations for the safeguarding, accounting, and auditing of all monies received and derived from extraclassroom activities. The Regulations require the board to appoint a central treasurer responsible for extra-classroom activities fund receipts and disbursements and a central auditor to oversee management of the extra-classroom activities funds.

Generally, extra-classroom activity funds are raised through charges for, by, or in the name of organizations whose activities are conducted by students. Students raise and spend these funds to promote the general welfare, education, and morale of all students, and to finance the normal and appropriate extracurricular activities of the student body. The District's 20 accounts in the extra-classroom activity fund (activity fund) recorded more than \$563,000 in receipts and disbursements during the period July 1, 2005 to June 30, 2007 and had a combined cash balance of approximately \$72,000 as of June 30, 2007.

The Board and District officials are responsible for protection and oversight of the District's cash assets, including activity fund monies. These responsibilities include adopting policies and procedures that describe the records that District personnel and students must maintain, and the duties and control procedures that they must follow to adequately safeguard activity fund monies. Having a good system of internal controls over these funds helps minimize the risk that errors or irregularities may occur and go undetected.

We found the Board had not adopted policies and procedures providing guidance and internal controls in regard to the extra-classroom activity fund. Additionally, the District had not appointed a faculty auditor to oversee the management of the fund. As a result, neither the Board nor District officials had assurance that activity fund monies were being properly accounted for in compliance with regulations.

As a result of the internal control weaknesses we identified, we reviewed 15 disbursements totaling \$23,585 remitted from 11 of the 20 activity fund accounts during the audit period to determine if the expenditures were made for appropriate student activities. Additionally, we scanned a sample of more than 400 cancelled checks and 300 cash receipts that were issued during our scope period in order

to verify that they were issued in sequence and could be accounted for. We noted no exceptions based on our testing.

We also examined 20 cash receipts totaling \$13,437 for nine activity fund accounts during the 2005-06 fiscal year to verify that the monies were deposited timely in accordance with good business practices. We found that for all 20 cash receipts it took 11 days or more from the date funds were received until they were deposited. For example, receipts totaling \$2,219.25 (including \$2,024.25 in cash) were collected on March 30, 2007 and March 31, 2007 and not deposited at the bank until 38 days later on May 8, 2007. When cash is not deposited promptly, it is subject to increased risk of loss or misuse.

District officials were unable to provide us with student activity deposit forms for the 2006-07 fiscal year. As a result, we were unable to test the timeliness of cash receipt deposits for the 2006-07 fiscal year. We interviewed the Deputy Central Treasurer who indicated the student activity deposit forms had been misplaced for the 2006-07 fiscal year, and thus we could not determine the time period from the date funds were received by the students to the time they were turned over to the Deputy Central Treasurer. However, we were able to determine the Deputy Central Treasurer had received funds, issued receipts and made the corresponding bank deposits. Fund raising records generated by extra-classroom activity fund activities are required to be retained for six years and the lack of such records could result in errors and irregularities occurring and not being detected by school officials.

Although we did not find that activity fund monies had been used inappropriately, the Board and District officials should take appropriate steps to better account for activity fund monies and to comply with the Commissioner's Regulations. Unless the Board increases its oversight of fund assets and District officials perform fund management duties in accordance with the Regulations and good business practices, there is a greater likelihood that errors and irregularities could occur and remain undetected and that activity fund monies could be misused.

## **Recommendations**

1. The Board should establish policies and procedures for the extra-classroom activity fund covering the duties, records, procedures and oversight required to ensure that all extra-classroom activity moneys are adequately safeguarded and used as intended.
2. The District should appoint a faculty auditor to oversee the management of extra-classroom activities fund moneys in accordance with requirements in the Regulations.

3. District officials should ensure that cash and checks collected for extra-classroom activities are deposited timely.
4. The Board should ensure that all fundraising records generated by extra-classroom activity fund activities are maintained by the District for six years.

# Information Technology

The District relies on an information technology (IT) system for computer education, access to the Internet, e-mail communication, storing student data, maintaining financial records and reporting to various State and Federal agencies. Therefore, the IT system and the data it holds are a valuable resource. If the IT system fails, the results could range from inconvenient to catastrophic. Even small disruptions in electronic data systems can require extensive employee and consultant hours to evaluate and repair.

The Board and District officials should control and monitor both user access and physical access to IT systems to reduce the risk of misuse and/or alteration of data and a potential financial loss to the District. The Board should also develop a formal disaster plan to provide guidance on the prevention of the loss of computer information as well as the recovery of data in the event of disaster. We found that internal controls over the District's fiscal management system and network were inadequate: computer equipment was not protected from unauthorized access; audit logs were not in place; backups of data were not adequately stored; and the District did not have a formal IT disaster plan. Because the Board did not develop policies and procedures to address these issues, the District's IT systems and electronic data have been subject to an increased risk of loss or misuse.

## Computer System Access

Access controls should provide reasonable assurance that computer resources are protected from unauthorized modifications. To control electronic access, a computer system or application needs a process in place to identify and differentiate among users. User accounts identify users and establish relationships between a user and a network, computer, or application. These accounts are created by the technology coordinator and contain information about the users, such as passwords and access rights to files, applications, directories and other computer resources. Access controls include establishing adequate passwords, limiting administrator accounts, and restricting users to only the applications<sup>1</sup> that are necessary for their day-to-day operations.

Passwords – Passwords are used to identify and authenticate a user when attempting access to a District's computer system or

---

<sup>1</sup> The District uses DOS-based financial software applications to process payroll and maintain employee leave accrual records, and Windows-based financial software applications to process all other financial transactions.

application. The more complex a password, the better the chances are that unauthorized users will be prevented from obtaining access to the system. As passwords can be guessed, copied, or overheard, passwords should be held to complexity requirements, password changes should be enforced on a periodic basis, and access rights revoked upon a set number of failed sign-on attempts. Using these techniques significantly increases the District's protection in preventing unauthorized users from accessing sensitive information.

The District's technology coordinator provides both students and employees with a password when they are first given access to the network. Once granted access to the network, students and employees are not required to change passwords periodically. Additionally, access rights are not revoked upon a set number of failed sign-on attempts.

We also noted that the District's payroll and leave accrual financial applications do not require passwords to access the applications. Currently, the School Business Executive, Deputy Treasurer, and payroll clerk have access to both applications. As a result, if these employees are signed into their computers, anyone could access the payroll and leave accrual financial software applications through an unattended workstation.

Additionally, we noted that the tax collector, School Business Executive, Deputy Treasurer, and payroll clerk have access to the application used for maintaining records of tax collection. Although passwords are required to access the application, the passwords are basic and lack any complexity requirements. Additionally, once users are assigned access to the application, they are not required to change passwords periodically and access rights are not revoked upon a set number of failed sign on attempts. We also found that all four individuals with access to the application use the same user name and password, both of which are identical.

We noted that the financial software applications used to process all other financial transactions contains a password field to access the applications. However, we found that the School Business Executive, Deputy Treasurer, and payroll clerk have not established a password within the system, and thus these individuals are capable of accessing the software application without the use of a password. Furthermore, the lack of a password increases the risk that unauthorized individuals could access the system through these employees' workstations.

User Rights Controls – To ensure proper segregation of duties and internal controls, the financial management system should only allow users to access the computer functions necessary to fulfill their job responsibilities. Having access controls in place prevents users from being involved in multiple aspects of financial transactions. Generally, a system administrator is designated as the person who has oversight and control of the system, and the ability to add new users as well as change users' passwords and rights. With this ability, administrators are able to control and use all aspects of the software. A good system of controls requires that this position be separate from the Business Office function.

The District's payroll, leave accrual, and tax collection financial software applications do not have access controls. As a result, the applications do not allow for the ability to restrict the access level of different users, which allows users of the application to have full access to all levels of the application. Currently, the School Business Executive, Deputy Treasurer, and payroll clerk have access to the payroll and leave accrual software applications, although only the payroll clerk's job responsibilities entail processing payroll and/or leave accrual transactions on a day-to-day basis. Additionally, these three individuals and the tax collector have access to the tax collection software application, although only the tax collector's job responsibilities entail maintaining records of tax collection on a day-to-day basis.

The software applications used to process all other financial transactions have access controls. The four access categories allowed are "All Access," "Some Access," "Read Only," and "No Access." The ability to restrict the access levels of different users is a good control feature in the computerized financial software applications. However, we found that the School Business Executive, Deputy Treasurer, and payroll clerk have "All Access" rights to the primary financial application, although access to all computer functions within the application is not required for them to be able to fulfill their day-to-day responsibilities. The School Business Executive and payroll clerk have access that enables them to create cash receipts, purchase orders, and vendors, although these functions are not needed for them to fulfill their day-to-day job responsibilities. Furthermore, the Deputy Treasurer has access that enables her to create journal entries and make budget transfers, although these functions are not needed for her to fulfill her day-to-day job responsibilities.

Additionally, we found that the School Business Executive has administrative rights to the District's financial software applications, which allows him the ability to add new users as well as change

users' passwords and rights. With this ability, the individual is able to control and use all aspects of the financial software applications, which creates the opportunity for the manipulation and concealment of transactions.

Based on the weaknesses noted over the District's fiscal management software, we performed a variety of tests of payroll payments, maintenance of leave accruals, and accounts payable payments, to verify that transactions during the audit period were appropriate. Our testing did not reveal any material exceptions.

### **Audit Logs**

A computerized fiscal management system should provide a means of determining, on a constant basis, who is accessing the system and what transactions are being processed. Audit logs (commonly known as audit trails) maintain a record of activity by system or application process. The audit log should provide information such as: (1) the identity of each person who has accessed the system, (2) the time and date of the access, (3) what activity occurred, and (4) the time and date of sign off. Ideally, this audit log or audit trail would be reviewed by management or management's designee, in order to monitor the activity of users who access the fiscal management software. This tool provides a mechanism for individual accountability, reconstructing events and problem monitoring.

Currently, the District's fiscal management software does not generate reports needed to properly monitor financial activity. Specifically, the software will not generate change reports showing, for example, vendor changes, or the addition or deletion of general and subsidiary ledger accounts. The software also does not have the ability to generate reports showing the identification of those who entered transactions into the system (audit logs). This is a significant weakness that could allow unauthorized activities to occur and go undetected and unresolved.

### **Physical Security Over Network Servers and Component Parts**

Maintaining adequate security over District IT systems helps to ensure that they are protected from loss and used effectively for their intended purpose. District officials can establish security over IT systems and equipment by controlling access to servers and components and by physically securing network components. However, we found that a network server and three wiring racks were not physically secured. Unauthorized individuals could gain access to these systems in the absence of staff in the rooms in which they are located. This could result in services being disrupted, costly equipment damaged, destroyed or stolen, and personal information being compromised.

## **Data Backup**

Data should be backed up (i.e., copy made) on a routine basis and the backup copy stored at an environmentally and physically secure off-site location. We found that District officials had not established policies or procedures for the backup of District information including the financial data. Currently, District financial data is backed up to an off-site network server on a daily basis. However, non-financial data residing on a network server in the high school/middle school is backed up to a server located within the same building. The technology coordinator also indicated that backups have not been periodically tested to verify the capability of restoring the District's system. If the system were to become compromised and a backup was not available to restore it to normal operations, the District risks losing most, if not all, of its computer-processed data.

## **Disaster Recovery**

The District's internal control system should include a formal disaster plan to address the possible loss of computer equipment and data and establish procedures for recovery in the event of such a loss. The plan should detail the precautions to be taken to minimize the effects of any disaster and enable the District to either maintain or quickly resume its mission-critical functions. The plan should include a significant focus on disaster prevention. However, the Board has not established a formal disaster plan and consequently, in the event of a disaster, District personnel have no guidelines or plan to follow to help minimize or prevent the loss of equipment and data or guidance on how to implement data recovery procedures.

## **Recommendations**

5. District officials should adopt policies and procedures to strengthen internal controls relating to the use of complex passwords, enforcement of password changes on a regular basis, and the revocation of access rights after a set number of failed sign on attempts.
6. District officials should ensure all financial software applications include requirements for strong passwords to access the system, the implementation of access controls, and the creation of audit logs to enable District officials to monitor user activity.
7. District officials should evaluate employee job descriptions and assign computer system access rights to match the respective job functions.
8. The Board should designate the responsibility for assigning user access rights to the fiscal management system to someone independent of the Business Office operations.
9. District officials should store backups of District information at an environmentally and physically secure off-site location.

In addition, this data should be periodically tested to verify it is capable of restoring the District's system.

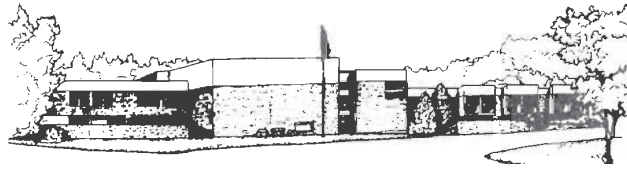
10. The Board should adopt policies and procedures to strengthen internal controls relating to IT equipment storage, computer backup and disaster recovery.

## **APPENDIX A**

### **RESPONSE FROM DISTRICT OFFICIALS**

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

Paul D. Savage II  
Superintendent  
1273 Rte. 9N  
Clintonville, NY 12924  
(518) 834-2845  
(518) 834-2843 (fax)



Scott A. Brow  
School Business Executive  
1273 Rte. 9N  
Clintonville, NY 12924  
(518) 834-2867  
(518) 834-9188 (fax)

## AuSable Valley Central School District

November 26, 2007

NYS Comptroller's Office  
Glens Falls Regional Office  
One Broad Street Plaza  
Glens Falls, NY 12801

Re: District Response To Audit

To Whom It May Concern,

The AuSable Valley Central School would like to thank the Comptroller's Office for a thorough and complete audit. The District is very pleased with the results of the audit. The audit indicates that the District is in overall good financial shape with no improprieties. The audit reported comments and recommendations in two areas, Extra-classroom Activity and IT Controls.

### **District Response to Recommendations 1-4, Extra-Classroom Activity**

The audit report makes recommendations relating to the management of extra classroom activity funds. Extra classroom activity funds are funds raised through charges for, by or in the name of organizations whose activities are conducted by students.

The District's activities fund has 20 accounts and the auditor's testing found no evidence that activity fund monies had been used inappropriately. Nevertheless, the report makes a series of recommendations to assist the Board and District officials in better accounting for activity fund monies and to comply with Commissioner's regulations.

The Board intends to establish policies and procedures for the classroom activity fund, using as a model the policies and procedures set forth in the Commissioner of Education's Finance Pamphlet #2, entitled "The Safeguarding, Accounting, and Auditing of Extra Classroom Activity Funds."

In accordance with the recommended policies and procedures, the District intends to appoint a faculty auditor to oversee the management of the extra classroom activity funds, and, through the recommended policies and procedures will take steps to ensure that cash and checks collected for extra classroom activities are deposited in a timely manner and that fundraising records are maintained by the District for six years.

**"Together We Make A Difference"**

### District Response to Recommendations 5-10, IT Controls

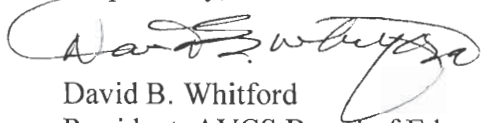
The audit report also included recommendations for improving the information technology system for computer education, access to the internet, e-mail communications, storing student data, maintaining financial records and reporting to various State and Federal agencies. The recommendations included developing a formal disaster plan to provide guidance on the prevention of the loss of computer information, as well as recovery of data in the event of a disaster, plus additional internal controls over the District's fiscal management systems. The District intends to improve in both of these areas. Historically, the District has focused its limited IT budget on maximizing educational applications for information technology. Based upon the recommendations, the District will improve its policies and practices with regard to disaster recovery, data backup, and improving computer system access.

The District intends to review model policies and procedures, and adopt appropriate policies to strengthen internal controls in the area of security measures. The District will also review functions of various software systems, and match access rights to job functions. The District will also seek to create and maintain audit logs.

The District will also explore options for data backup and disaster recovery, and take steps to designate the responsibility for assigning user access rights to someone independent of the business office operations. Finally, the Board will ensure that there are adequate policies and procedures in place to strengthen internal controls relating to IT equipment storage, backup, and disaster recovery.

Overall, the District is pleased with the current practices it has in place, and intends to submit to the Comptroller, within 90 days, a plan indicating how it intends to fully comply with the recommendations of the audit report. We appreciate the in depth examination of District policies, practices and procedures, and look forward to having the opportunity to continually improve our practices. However, it is gratifying to know that the District has avoided financial improprieties and that our community education dollars are being spent on education.

Respectfully,



David B. Whitford  
President, AVCS Board of Education

## 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: 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 upon the reported objectives and scope by selecting for audit those areas most at risk. We selected internal controls over extra-classroom activities and information technology for further audit testing.

Within extra-classroom activity funds, we reviewed all District policies relating to extra-classroom activities. We interviewed the central treasurer and deputy central treasurer of the activity fund, observed transactions, and examined extra-classroom activity fund records such as the central treasurer's ledger, payment order forms, cancelled checks, bank statements, validated deposit slips, student activity deposit forms, cash receipts, and cash receipts book, to determine the effectiveness of internal controls over extra-classroom activity fund functions and any associated effects of deficiencies in those controls.

Within information technology, we reviewed all District policies related to computer use and information technology. We interviewed the District's technology coordinator and system administrator specifically regarding network passwords, physical access to the system, controls within the fiscal management software, backups of data, and disaster recovery plans. We physically inspected the location of system equipment and viewed Business Office employees' computer screens to determine the software that each employee had access to. Additionally, we examined the following records and reports: purchase orders, claims packages, warrants, payroll journals, payroll transaction reports, personnel files, Board minutes, collective bargaining agreements and individual employment contracts, leave accrual summaries, timesheets, cancelled checks, cash receipts, and bank reconciliations.

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

## 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, Room 1050  
Buffalo, New York 14203-2510  
(716) 847-3647 Fax (716) 847-3643  
Email: [Muni-Buffalo@osc.state.ny.us](mailto:Muni-<u>Buffalo@osc.state.ny.us</u>)

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](mailto:Muni-<u>Rochester@osc.state.ny.us</u>)

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](mailto:Muni-<u>Syracuse@osc.state.ny.us</u>)

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](mailto:Muni-<u>Binghamton@osc.state.ny.us</u>)

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](mailto:Muni-<u>GlensFalls@osc.state.ny.us</u>)

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](mailto:Muni-<u>Albany@osc.state.ny.us</u>)

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

**HAUPPAUGE REGIONAL OFFICE**

Richard J. Rennard, 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](mailto:Muni-<u>Hauppauge@osc.state.ny.us</u>)

Serving: Nassau, Suffolk counties

**NEWBURGH REGIONAL OFFICE**

Christopher Ellis, Chief Examiner  
Office of the State Comptroller  
33 Airport Center Drive, Suite 103  
New Windsor, NY 12553-4725  
(845) 567-0858 Fax (845) 567-0080  
Email: [Muni-Newburgh@osc.state.ny.us](mailto:Muni-<u>Newburgh@osc.state.ny.us</u>)

Serving: Orange, Putnam, Rockland, Westchester  
counties