



Avoca Central School District Safeguarding Cash Assets and Information Technology

Report of Examination

Period Covered:

July 1, 2006 — October 1, 2007

2008M-39



Thomas P. DiNapoli

Table of Contents

	Page
AUTHORITY LETTER	3
EXECUTIVE SUMMARY	5
INTRODUCTION	7
Background	7
Objective	7
Scope and Methodology	8
Comments of District Officials and Corrective Action	8
CASH ASSETS	9
Signature Disk	9
Online Banking	10
Check Images	11
Recommendations	11
INFORMATION TECHNOLOGY	12
Access Rights	13
Exception and Change Reports	13
Disaster Recovery Plan	14
Recommendations	14
APPENDIX A Response From District Officials	16
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

May 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 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 Avoca Central School District, entitled Safeguarding Cash Assets and Information Technology. 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 Avoca Central School District (District) is governed by the Board of Education (Board) which comprises five 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. The Treasurer/Business Manager (Treasurer) is the custodian of District moneys and is responsible for cash disbursements and deposits. The duties of the District Clerk (Clerk) include bank reconciliation.

At June 30, 2006, the District had approximately \$4 million on deposit in more than 30 bank accounts at two area banks. District personnel use a signature disk to affix the Treasurer's electronic signature to checks, and bank reconciliations are performed using scanned images of the cancelled checks. The Treasurer uses online banking to facilitate the District's financial operation. The Treasurer also administers the District's financial software, purchased from the Board of Cooperative Educational Services (BOCES) Western New York Regional Information Center (WNYRIC).

Scope and Objective

The objective of our audit was to assess the District's internal controls over its cash assets and information technology functions for the period July 1, 2006 to October 1, 2007. Our audit addressed the following related questions:

- Are internal controls over cash appropriately designed and operating effectively to adequately safeguard District assets?
- Are internal controls over employees' access rights to the District's financial software and over District information technology (IT) resources appropriately designed to adequately safeguard District assets?

Audit Results

The Board did not establish proper internal controls to ensure that cash assets are safeguarded, and District officials did not develop procedures for doing so. The Treasurer does not directly oversee the use of her signature disk at all times, and the disk is not password-protected. The payroll clerk and accounts payable clerk both use the Treasurer's signature disk to sign District checks without the Treasurer's direct oversight. Online banking transactions made by the Treasurer are not independently reviewed or confirmed by another District employee. Additionally, the bank returns only the front

image of the District's cancelled checks rather than both the front and back as required by law, preventing the proper reconciliation of bank statements. Because of these control weaknesses, District officials do not have adequate assurance that signed checks are for legitimate District purposes, and there is an increased risk of checks being altered and/or improperly presented to the bank without being detected.

The Board did not effectively address the safeguarding of the District's information technology assets, including computer data, equipment, and media. The Board has not adopted comprehensive policies and procedures to ensure that access to the District's financial software is restricted to only those functions required by individual employees' job duties, therefore not preserving the proper segregation of duties on the system. District officials do not review the exception reports and change reports provided with their financial software to monitor employees' activities on the system in order to detect unauthorized or unusual activity. Further, District officials did not establish a formal disaster recovery plan and procedures to address potentially disastrous events that may cause the loss of critical functions or data. The lack of comprehensive policies and procedures related to information technology puts the District's data, network, and applications at an increased risk of damage or loss, and exposes the District's critical business functions to the risk of costly disruption.

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 plan to initiate corrective action.

Introduction

Background

The Avoca Central School District (District) is located in the Towns of Avoca, Wheeler, Prattsburgh, Howard, Fremont, Cohocton, and Bath, in Steuben County. The District is governed by the Board of Education (Board) which comprises five 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. The Treasurer/Business Manager (Treasurer) is the custodian of District moneys and is responsible for cash disbursements and deposits.

There is one school in operation within the District, with approximately 575 students. The District's operating expenditures for the 2006-07 fiscal year were approximately \$9 million and were funded primarily with State aid, real property taxes, and grants.

At June 30, 2006, the District had approximately \$4 million on deposit in over 30 bank accounts at two area banks. District personnel use a signature disk with the Treasurer's signature to electronically sign District checks. The bank returns check images to the District instead of the actual cancelled checks. The Treasurer uses online banking to facilitate the District's financial operation.

The District uses financial software purchased from the Board of Cooperative Educational Services (BOCES) Western New York Regional Information Center (WNYRIC). The Treasurer administers the software, and BOCES provides the District with an on-site technician who is a BOCES employee, has a supervisor at the BOCES, and answers to the District's elementary school Principal.

Objective

The objective of our audit was to assess the District's internal controls over its cash assets and IT functions. Our audit addressed the following related questions:

- Are internal controls over cash appropriately designed and operating effectively to adequately safeguard District assets?
- Are internal controls over employees' access rights to the District's financial software and over District IT resources appropriately designed to adequately safeguard District assets?

**Scope and
Methodology**

We examined the internal controls of the Avoca Central School District for the period July 1, 2006 to October 1, 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 plan 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*.

Cash Assets

The Board is responsible for establishing internal controls to ensure that the District's cash assets are adequately safeguarded. Such controls include policies and procedures requiring that cash disbursements are properly authorized and documented, and that banking transactions – including those conducted online – are appropriately controlled and monitored. Written policies and procedures help to ensure that District personnel who perform banking transactions understand the Board's overall goals, and provide specific guidance for meeting those goals. For example, the use of electronic signatures must be supervised by the appropriate official, online banking duties and authorizations must be clearly defined and independently reviewed, and check images used in bank statement reconciliations should comply with legal requirements.

The Treasurer is the custodian of District moneys and performs duties that include printing and signing checks. At its annual reorganization meeting, the Board designates the financial institutions the District will use, and also designates a secondary signatory to prepare and sign checks should the Treasurer not be able to do so. Both the payroll clerk and the accounts payable clerk also issue checks using the District's financial software, which applies the Treasurer's electronic signature. Bank reconciliations are performed by the District Clerk using check images returned by the District's banks.

We found that the Board had not adopted policies for the adequate safeguarding of the District's cash assets, and District officials did not develop procedures to guide District personnel in meeting policy requirements. Specifically, there were no written procedures for the protection and use of electronic signatures, or for the appropriate assignment and review of online banking transactions. Additionally, the check images that the District Clerk used to reconcile the District's bank statements did not include both the fronts and backs of the checks, as required by law. These control weaknesses place the District's cash assets at an increased risk of mismanagement, misuse, or loss.

Signature Disk

As the District official responsible for signing checks, the Treasurer must ensure that her signature is not used to make payments that have not been approved. Education Law requires the actual or a facsimile of the Treasurer's signature to be applied to District checks either by the Treasurer or under the Treasurer's direct supervision. Other appropriate controls include the use of unique passwords by the Treasurer and staff who use the signature disk. Such controls are

especially important when individuals authorized to use the signature disk can also modify employee information in the District's financial system.

The Treasurer's signature disk is locked in the safe in the Business Office when not in use. To print checks from the financial software with the Treasurer's signature, the disk must be inserted into the computer from which the checks are printed. The Treasurer did not directly oversee all use of the signature disk, and the disk was not password-protected. The payroll clerk and accounts payable clerk both had access to the safe where the disk was kept, and used the disk on their computers to apply the Treasurer's signature to checks and print them without the Treasurer's direct oversight. Both the payroll clerk and the accounts payable clerk also had the ability to add, edit, and delete employee information in the accounting software. The weak controls over the signature disk, combined with the clerks' ability to change employee information, create increased opportunities for employees to use the Treasurer's signature inappropriately without being detected.

To address this risk, we traced 25 transactions from cancelled checks to bank statements, approved warrants, and supporting voucher packets, and found no irregularities. However, the absence of comprehensive policies and procedures for the control and use of signature disks, and the Treasurer's lack of control over the use of the signature disk, increase the risk that her signature could be used inappropriately and that errors or irregularities could occur without being detected.

Online Banking

Online banking offers District personnel the capability to review and verify District transactions and bank balances on a current basis, in conjunction with the use of printed statements from the District's financial institutions. Additionally, online banking can include financial transactions with District vendors and other institutions external to the District. Good business practices require that transactions initiated online are verified by the banking institution with someone at the District other than the individual initiating the transaction, and that supporting documentation is available for review by an independent District official. Alternatively, District officials can limit the use of online services to informational purposes only, such as verifying cleared checks, without permitting any online transactions. In either case, effective controls over online banking include written policies and procedures to guide personnel in performing online banking activities.

The Board did not adopt written policies addressing online banking, and District officials did not develop specific procedures, leaving

Business Office personnel without adequate guidance in the use of this service. The Treasurer was the only employee with access to online transfers, and could make online transfers among accounts within the same bank, as well as transfers to external bank accounts, without independent review or verification by another District official.

Accordingly, we tested five online transfers¹ totaling \$125,535 from bank statements to supporting documentation. Although our audit found no irregularities, the District will continue to be at risk for improper online bank transfers occurring and going undetected, unless the Board adopts online banking policies and District officials implement related procedures to control this banking activity.

Check Images

Good business practices dictate the thorough reconciliation of bank accounts on a regular basis. This includes reconciling bank balances to account balances and individual transactions, as well as reviewing cancelled checks for correct amounts, payee information, and appropriate signatures. A proper review of cancelled checks includes both the front and the back of the checks, because the back of a check shows endorsement information. Further, General Municipal Law requires that if a district receives images in lieu of the actual cancelled checks, both the front and the back must be imaged.

The District requested and received images of only the front of its checks, and the Treasurer stated that District officials were unaware of the legal requirements. To test for accuracy and proper authorization, we traced 15 transactions from cancelled checks to bank statements, approved warrants, and supporting voucher packets. Though our audit found no irregularities, the District Clerk did not have the imaged backs of checks to aid in the proper reconciliation of the bank accounts. Therefore, the District is not in compliance with General Municipal Law requirements and is at an increased risk of not detecting checks that were altered and/or improperly presented to the bank.

Recommendations

1. The Treasurer should control the signature disk and directly oversee its use.
2. The Board should adopt written policies to require pre-authorization of online transfers and properly itemized documentation of the transfers.
3. The Treasurer or District Clerk should ensure that the District's banks provide complete check images of cancelled checks, including the backs of the checks with the fronts.

¹ These transfers moved moneys from one fund to another to cover expenditures.

Information Technology

District management relies on its information technology (IT) system to maintain financial and student data, process financial transactions, provide computer education, access the Internet, communicate by electronic mail (email), and report to State and Federal agencies as well as to the general public. The potential consequences of a system failure can range from inconvenient to severe; even small disruptions in processing can require extensive time and effort to evaluate and repair. Computerized personal data can also be a potential liability to the District if lost or improperly disclosed. Accordingly, District officials are responsible for establishing internal controls to provide reasonable assurance that the District's valuable IT assets – including computer data, equipment, systems, and media – are properly used and safeguarded against waste, loss, and misuse. Such controls include:

- User Access Rights – Evaluation and assignment of permissions so that users can access only those areas of the system they need to perform their jobs
- Exception and Change Reports – Routine review of system-generated reports that track individuals' activities on the system
- Disaster Recovery Plan – Development of a formal plan that includes precautions to minimize the potential loss of data, and steps that District personnel should take to restore lost data and resume critical operations as quickly as possible in the event of a disaster.

The District uses a financial software package purchased from the Board of Cooperative Educational Services (BOCES) Western New York Regional Information Center (WNYRIC). The Treasurer administers the software, and BOCES provides the District with an on-site technician who is a BOCES employee, has a supervisor at the BOCES, and answers to the District's elementary school Principal. The software includes accounting, budget, payroll, human resources, and negotiations modules, and is installed on four computers in the District office. The Treasurer, payroll clerk, accounts payable clerk, and District Clerk all have access to the financial software.

District officials did not establish policies and procedures to effectively safeguard the District's computer systems and data. Specifically, our audit disclosed weaknesses in controls over the

computerized financial system with regard to assigning access rights, monitoring of activity reports, and disaster recovery planning.

Access Rights

Effective controls over users' access to computer operations restrict authorizations to only those functions needed for individuals to perform their job duties, and ensure that such access prevents them from being involved in multiple aspects of a financial transaction. In this way, system access controls help to preserve the proper segregation of duties. The Board is responsible for adopting policies to ensure that access rights to the District's IT resources are appropriately restricted, and District officials must develop procedures for that purpose.

The District did not have a written policy and procedures addressing access rights. Additionally, District employees told us that the District's teachers had partial system administrative rights, enabling them to download and install software that may not be adequately screened for viruses, or may not be used for valid District purposes. Further, users' access rights to the District's financial software did not support an adequate segregation of duties. All four users had access to the human resources module (although the Treasurer's access was limited to read-only). The Treasurer, payroll clerk and accounts payable clerk all had the ability to print accounts payable checks, and the Treasurer had full administrative rights including the ability to change and delete files and establish employees' user access rights. Lastly, all four users were granted override capabilities for purchase orders and cash disbursements.

Due to the lack of guidance from the Board, individuals charged with establishing and handling the District's information technology resources have granted users more access rights than necessary to perform their jobs. This has placed the District's IT resources at an increased risk of loss, damage, or inappropriate disclosure through the accidental or deliberate actions of unauthorized users.

Exception and Change Reports

A good financial software package provides adequate tools for the District to establish strong internal controls over the use of its financial applications. Exception reports and change reports are two basic tools that are commonly available. Exception reports are detailed lists of transactions that may be exceptions to ordinary transactions; change reports show changes made to certain data records, such as vendor or personnel information. These reports are effective aids for management to establish accountability for employees' use of District computers and identify potentially erroneous or improper activities. Board policies should express the Board's objectives for the financial system's capabilities, and written procedures should outline the steps for maximizing those

capabilities, including the use of available automated controls such as exception and change reports.

The Treasurer, who also administers the District's financial system, indicated that she was unaware of the availability of exception and change reports in the District's financial software, and that the Board did not establish policies and procedures for their use. Without the routine review of these monitoring tools, internal controls over employees' use of the financial software and the safeguarding of District data are weakened, particularly when the assigned user access rights do not support an adequate segregation of duties (see "Access Rights," above). As a result, the District's valuable financial information is at an increased risk of loss or misuse.

Disaster Recovery Plan

The District's IT system – including equipment, software, and data – is a critical resource that must be adequately protected against loss, damage, or misuse. An effective internal control system for IT requires a formal disaster recovery plan to prevent the potential loss of computer resources, and to outline procedures for the recovery of data in the event of a disaster. A Disaster Recovery Plan (DRP) – sometimes referred to as a Business Continuity Plan (BCP) or Business Process Contingency Plan (BPCP) – describes how an organization should deal with potential disasters. Such a plan includes precautions to minimize the effects of a disaster and to enable the organization to either maintain or quickly resume mission-critical functions. Typically, disaster recovery planning involves an analysis of business processes and continuity needs, and may also include a focus on disaster prevention. The routine backup of the District's software and data is one element of effective disaster recovery planning.

The Board did not establish formal policies and procedures to address disastrous events that may result in the loss of critical functions, equipment, and/or data. Although District personnel performed routine backups of the District's data, without a formal Disaster Recovery Plan they have no written guidelines to restore essential operations if a catastrophic event were to occur. As a result, the District is at a significant risk of incurring costly disruptions to its business operations, and of losing critical equipment and/or data with no ability to recover functionality.

Recommendations

4. The Board should adopt written policies and the Treasurer should develop procedures addressing the appropriate assignment and restriction of user access rights.
5. The Board should adopt written policies and the Treasurer should develop procedures for routine management review of system-

generated exception and change reports to detect unusual or inappropriate activities on the District's financial system.

6. The Board should adopt written policies and the Superintendent should develop procedures regarding disaster recovery. These procedures should include the development of a formal, comprehensive disaster recovery plan.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

Administration

Superintendent,
R. Christopher Roser

7 – 12 Interim Principal
Robert Codispoti

K – 6 Principal
Richard Yochem

District Treasurer
Gay Fairbrother



17-29 Oliver Street, Avoca, NY 14809
(607) 566-2221

Board Of Education

President, Mary Ellen Johnson

Vice President, David Dockstader

Michael Slayton

Brian Patterson

Rachael McLoud

May 2, 2008

Office of the State Comptroller
110 State Street
Albany, New York 12236

To whom it may concern:

On April 7, 2008 we received the draft audit report, and as a result of the findings we are proposing the following action plan:

1. The Treasurer should control the signature disk and directly oversee its use.

► We are pleased that when you traced a sampling of transactions from cancelled checks to bank statements, approved warrants, and supporting voucher packets, no irregularities were found. In order to eliminate the increased risk that the signature disk could be used inappropriately in the future, a draft policy has been developed for the approval of the Board of Education. The accompanying regulation has also been developed and actually was implemented prior to the District's receipt of this report.

2. The Board should adopt written policies to require pre-authorization of online transfers and properly itemized documentation of the transfers.

► We are again pleased that during your test of online transfers no irregularities were found. However, to eliminate the risk for improper transactions in the future, a draft policy has been developed for the approval of the Board of Education. The accompanying regulation has been developed as well.

3. The Treasurer or District Clerk should ensure that the District's banks provide complete check images of cancelled checks, including the backs of the checks with the fronts.

► This was corrected during the course of the audit. Beginning with the December 2007 bank statements, both the front and the back of the cancelled checks are imaged and included.

4. The Board should adopt written policies and the Treasurer should develop procedures addressing the appropriate assignment and restriction of user access rights.

► A policy and accompanying regulations have been developed concerning Financial Management Software Administration. The district officials have reviewed the access rights of employees using the district's financial software. User rights will be restricted to only those rights necessary for an employee to perform his or her job. The Technology Coordinator will be designated the responsibility of assigning user access rights to the financial software. The Technology Coordinator is independent of the Business Office operations. This will eliminate the Treasurer's ability to change and delete files and to change her own or others' user access rights. The Treasurer's ability to print accounts payable checks and access to the human resources module will be disabled. Since the District is in the process of training the accounts payable clerk to take over for the payroll clerk upon her retirement in October 2008, we feel it is necessary for both employees to have access to certain portions of the human resources module, the payroll module and the accounts payable functions of the system. The district clerk will continue to have access to certain portions of the human resources module necessary to add new district employees.

5. The Board should adopt written policies and the Treasurer should develop procedures for routine management review of system-generated exception and change reports to detect unusual or inappropriate activities on the District's financial system.

► The same policy, Financial Management Software Administration addresses the subject of various Exception and Change Reports. Our financial management software gives our district the ability to manage passwords, monitor user log-ins, track changes of vendor payment names, compare changes to payroll, and log user activity related to changed data via full system audit reports. Since we are such a small district, in order to further reduce the risk of erroneous or improper activities, it is necessary for the Treasurer to review changes to vendor payment names and compare changes to payroll and the Superintendent or his designee to review the System Audit Reports on a weekly basis.

6. The Board should adopt written policies and the Superintendent should develop procedures regarding disaster recovery. These procedures should include the development of a formal, comprehensive disaster recovery plan.

► A policy and accompanying regulation concerning Computer Control for Financial Network and District Computer Systems, has been developed and will be presented to the Board of Education for review. A formal comprehensive disaster recovery plan will be developed during the 2008-2009 school year.

Respectfully Submitted,



R. Christopher Roser
Superintendent of Schools

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 banking transactions and information technology for further audit testing.

Our testing included the following:

- We verified and traced a sample of bank transfers for accuracy and proper approvals.
- We traced selected financial transactions to the cancelled checks and back to the supporting voucher packets, and tested for proper approvals and consistency.
- We traced selected cash receipt transactions to the cash receipts journal, bank statements, and deposit slips.
- We interviewed pertinent staff about policies and procedures relating to banking transactions and information technology.
- We inquired about specific internal controls relating to banking transactions and information technology.

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

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