OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT & SCHOOL ACCOUNTABILITY

Town of Hartford

Online Banking and Information Security

Report of Examination

Period Covered:

January 1, 2015 – July 31, 2016

2016M-385

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

February 2017

Dear Town Officials:

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

Following is a report of our audit of the Town of Hartford, entitled Online Banking and Information Security. 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 New York State General Municipal Law.

This audit's results and recommendations are resources for local government 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 Town of Hartford (Town) is located in Washington County and has a population of approximately 2,270 residents. The Town is governed by an elected five-member Town Board (Board), which consists of the Town Supervisor (Supervisor) and four councilpersons. The Board is responsible for the general oversight of the Town's operations and finances.

The Town provides various services to its residents, including highway maintenance, snow removal and general governmental support. These services are financed primarily by real property taxes and State aid. Total budgeted appropriations for 2016 are approximately $1.1 million.

The Town's electronic accounting records are maintained by the Supervisor's Accounting Clerk (Clerk) who is also the Budget Officer. In addition to maintaining the accounting records on a computer system operated independently from the Town,[1] the Clerk prepares the payroll along with the online transmission of bi-weekly payroll direct deposit payments, preparation of checks for all payments, electronic bank transfers between Town bank accounts, and online banking payments. Total online transactions (excluding transfers between Town bank accounts) for January 1, 2015 through July 31, 2016 were $529,062.

Objective

The objective of our audit was to review online banking transactions and determine if the electronic financial information is adequately secured. Our audit addressed the following related question:

- Did the Board establish and implement adequate procedures over online banking and the security of electronic information to ensure the protection of the Town's assets and data?

Scope and Methodology

We examined the Town online banking transactions and electronic security of financial information of the Town for the period January 1, 2015 through July 31, 2016.

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. Unless otherwise indicated in this report, samples for testing were selected based on professional

[1] The Clerk processes and stores all of the Town's computerized accounting data at his accounting firm.

judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

Comments of Local Officials and Corrective Action

The results of our audit and recommendations have been discussed with Town officials, and their comments, which appear in Appendix A, have been considered in preparing this report. Town officials generally agreed with our recommendations and indicated they planned to initiate corrective action.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and forwarded to our office within 90 days, pursuant to Section 35 of General Municipal Law. 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. We encourage the Board to make this plan available for public review in the Clerk's office.

Online Banking and Information Security

Online banking provides direct access to moneys held in the Town's accounts. It is an immediate way to review current account balances and recent transactions, and to transfer moneys between bank accounts and to external accounts. General Municipal Law (GML) allows local governments to disburse or transfer funds in their custody by means of electronic or wire transfers. The Board must adopt an online banking policy and establish controls that provide for an adequate segregation of incompatible duties for initiating and authorizing online transfers, and for supervisory approval and bank confirmation. To the extent possible, the duties of authorizing, initiating and recording online transfers should be performed by different individuals. Online transfer confirmations from the bank should not be received by the same individual who initiates the transfers.

The Town relies on information technology (IT) systems for storing important information. Protecting the Town's electronic information is especially important given the rise in malicious attempts to harm computer networks or gain unauthorized access through viruses, malware and other types of attacks. The Board is responsible for ensuring that effective IT controls are in place by understanding how sensitive data is captured and stored, and by adopting and updating policies for disaster recovery plans and breach notification. Further, when computerized data is processed and stored at an external location not in the Town's control, the Board should enter into a written agreement with the party in control of the computerized data that states the Town's needs and expectations and specifies the level of service to be provided.

The Board has not established adequate procedures for online banking or the security of electronic information. The Clerk conducts all online banking transactions and manages the Town's electronic information at his private accounting firm. However, the Town does not have an online banking policy or a written agreement with his accounting firm or any third party used for IT services to outline the Town's needs and expectations and level of service required. Further, the Board has not developed computer security and disaster recovery plans.

Electronic Banking Transactions

Online wire or electronic transfers of funds can disburse amounts of money, usually within minutes of being executed. Therefore, to help prevent unauthorized transfers from occurring, it is important to control the processing of wire transfers. Policies and procedures for secure access to banking websites help to reduce the risk of unauthorized transfers from both internal and external sources. For example, using a dedicated computer to process all electronic

banking transactions can reduce such risk. Appropriate controls can also include requiring the bank to email or text a Town official (independent of the individual initiating the transfer) requiring their approval before an online transaction occurs. Proper segregation of duties is critical for managing transactions so that the authorization and transmitting functions are not assigned to the same person.

The Board is responsible for adopting an online electronic banking policy that specifies authorized transactions. This policy should define who can authorize and record transactions, and make transfers; who has access to online banking; and who will review and reconcile transfers. The policy should also identify the procedures for responding to potential fraudulent activity. Because there is a limited recovery window and a rapid response may prevent additional losses, bank accounts should be monitored at least every two to three days for unauthorized or suspicious activity.[2] In addition, the Board must enter into an agreement with the bank that provides the electronic banking services to ensure that the most current methods of protecting the Town's cash assets are in place during an electronic banking transaction.

The Board has not adopted an online banking policy that defines the process for authorizing, processing and monitoring transactions. While the Town has a banking agreement on file,[3] the Board did not know what controls the financial institution has implemented to protect the Town's cash assets or how the process was functioning. Furthermore, the Supervisor does not monitor the Town's online banking activity in a timely manner.

The Town uses online banking services to transfer funds between various Town accounts and to transfer funds to non-Town accounts for various purposes such as remitting employee payroll tax withholdings to government entities, transfers to employee Health Savings Accounts, sales tax payments, and other transfers to vendors such as employee payroll deductions for disability insurance. The Town's electronic banking transactions are authorized, processed and recorded in the Town's accounting records by the Clerk at his private accounting firm. Even though the Clerk is an employee, the Town does not provide him with a dedicated computer for electronic banking transactions; instead, he conducts Town banking transactions using one of his firm's computers. For accessing the Town's bank accounts, the bank provides a passcode by phone that allows the Clerk to view

[2] *Local Government Management Guide, Information Technology Governance*

[3] The Business Online Banking User Agreement between the Town and the bank was dated 2016.

transactions and perform transfers between Town bank accounts, and provides another layer of security codes to the Clerk for performing ACH transfers to other banks.[4] The Town is limited by the bank to a maximum transaction amount that can be processed. In addition, the bank sends an email notifying the Clerk of the electronic banking or ACH transfer processed. However, the bank does not call or email any other Town official who is not involved in the electronic banking process to provide notification of these transactions. When the duties of transaction authorization and processing are performed by the same individual who receives verification of those transactions, controls are weak and there is an increased risk of inappropriate transactions.

Additionally, the Supervisor does not authorize or monitor online banking transactions as they occur. Although the Supervisor reviews the monthly bank statements and reconciliations prepared by the Clerk by the last day of the following month, a routine review of all online banking transactions is an important control that can reduce the risk of unauthorized transactions.

We reviewed transfers between Town bank accounts and transfers to other entities to determine if the online transactions were authorized, supported and for a valid Town purpose. We tested 85 online transactions made to outside entities during six months, representing $159,435 out of a total of $529,062 during the audit period (30 percent), and found all the transactions were adequately supported and for a valid Town purpose. We also selected 95 transfers between Town bank accounts for the same period, totaling $541,073,[5] and determined those transfers were all for proper Town purposes. However, all the online transactions were completed by the Clerk without prior approval or verification by a separate Town official such as the Supervisor.

Although our audit found no evidence of inappropriate transactions, without comprehensive policies and procedures that adequately segregate incompatible duties and provide for timely monitoring of bank accounts, there is an increased risk that fraudulent or questionable online banking activity could occur and not be detected in a timely manner.

Security of Information

To properly protect the Town's computer resources, including sensitive data, the Board must be knowledgeable about those resources, how data is processed, and security provisions for sensitive data when it is processed, stored on backup or transferred electronically over

[4] ACH, or Automated Clearing House, is an electronic network used to process large volumes of electronic payments between banks.

[5] See Appendix B, Audit Methodology and Standards, for details on sample selection.

the Internet. When the Board relies on a third party to process and store the electronic financial information at a location other than Town facilities, it is important to enter into a written agreement with the third party to outline the needs and expectations and level of service expected. In addition, policies and procedures for the Town's computerized accounting data are part of the internal control system and provide criteria and guidance for the safeguarding of sensitive accounting and payroll data.

IT Service Contract — The Town relies on the Clerk's private accounting firm to provide a variety of IT-related services. For the Town's protection and to avoid potential misunderstandings, if the Town is not providing computer equipment and instead relying on the Clerk's firm for IT services, the Board should have a written agreement with the accounting firm or any third party providing IT services that clearly defines the services and information security to be provided. The lack of a written agreement, or a poorly worded agreement, can contribute to confusion over responsibility for various aspects of the IT environment (i.e., the accounting firm or Town officials), which puts the Town's data at greater risk for unauthorized access, misuse or loss. The Board should also be knowledgeable about how the data is processed and kept secure while being processed, stored on backup media or transferred electronically over the Internet.

Through inquiries of the Supervisor and one Board member, we determined that they do not have an understanding of how the Town's data is processed or what security measures are taken to protect sensitive data when it is processed, stored or transmitted at the accounting firm. There is no written agreement between the Town and either the Clerk's accounting firm, or any other party used to manage the Town's electronic information, that outlines the Town's needs and expectations and specifies the level of services to be provided.

The Clerk provides the Supervisor with accounting records that include hardcopy bank statements and reconciliations, payroll registers, federal/State payroll reporting forms, monthly budget-to-actual reports and retirement reports. However, the computerized accounting data and backups remain in the custody of the Clerk's accounting firm. Because Town officials are not sufficiently familiar with the Town's data processing and storage processes, there is an increased risk that Town personnel would be unable to recreate the accounting records or continue the Town's business operations in the event of a disaster or if the Clerk is unavailable.

Disaster Recovery Plan — A disaster recovery plan is intended to identify and describe how Town officials will deal with potential disasters. Such disasters may include any catastrophic event (e.g., fire,

computer virus or inadvertent employee action) that compromises the availability or integrity of the IT system and data. Contingency planning is used to avert or minimize the damage and impact that disasters would cause to operations. Such planning consists of precautions to minimize the effects of a disaster so officials and staff will be able to maintain or quickly resume day-to-day operations. Typically, a disaster recovery plan involves an analysis of business processes and continuity needs, including a significant focus on disaster prevention. The plan should also address the roles of key individuals, be distributed to all responsible parties, and be periodically tested and updated as needed.

The Board has not adopted a comprehensive disaster recovery plan to address potential disasters. Town officials told us that the Clerk adequately secures data and could retrieve it if the need arises. However, in the absence of the Clerk, Town personnel have no guidelines or plan to appropriately recover data if a disaster occurs. Without a comprehensive disaster recovery plan, the Town could lose important financial data and suffer a serious interruption in operations if a catastrophic event occurred. Further, because the Town has not entered into an agreement with the Clerk's firm for maintaining the Town's electronic data, the responsibilities related to disaster recovery are not clearly defined.

Breach Notification Policy — An individual's private and financial information, along with confidential business information, could be severely affected if the Town's computer security is breached or data is improperly disclosed. New York State Technology Law requires the Town to establish an information breach notification policy, which should detail how the Town would notify individuals whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. It is important for the disclosure to be made in the most expedient manner possible to accommodate the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and to restore data system integrity. The Board had adopted a breach notification policy in 2006 and is in the process of adopting an updated policy.

Recommendations

The Board should:

1. Adopt a policy for online banking and obtain an updated banking agreement with the Town's financial institution defining online banking security measures.

2. Consider providing, and requiring the use of, a dedicated computer for all online banking activities.

3. Ensure that bank accounts are actively monitored for unauthorized or suspicious activity by someone other than the Clerk.

4. Become knowledgeable about the Town's computerized data processing and the security of sensitive data when it is processed, stored on backup or transferred electronically.

5. Execute a written agreement with any third party that manages the Town's electronic information, stating the Town's needs and expectations and specifying the level of service to be provided.

6. Adopt IT policies and procedures for data security and disaster recovery.

APPENDIX A

RESPONSE FROM LOCAL OFFICIALS

The local officials' response to this audit can be found on the following page.

Hartford, the Heart of
Washington County

TOWN OF HARTFORD
PO Box 214
165 Hartford Main St.
Hartford, NY 12838
Town Phone#518-632-9151
Town Fax #518-632-9280
Town Web Site-www.hartfordny.com

To: NYS Comptroller's Office 2/16/17
Subj: Town of Hartford response to the NYS Comptroller's audit 2016M-385

The Town of Hartford is very satisfied that after having an audit that reviewed 19 months worth of Town activity from 1/1/15 to 7/31/16, there were no findings of any dubious or inappropriate conduct or transactions. The Town takes pride in the fact that the Comptroller's office affirms that the Town conducts its business in accordance with generally accepted government accounting standards.

The Town of Hartford acknowledges that it can update and improve our Information Technology practices and appreciates the Comptroller's office focusing on it, since no other detrimental findings were found for the Town to correct. Improving Information Technology and electronic data security is a goal every form of government can work on whether it be a small rural town like Hartford, or branches of the State and Federal government.

1. The Town of Hartford will consider adopting a policy for online banking. The Town did have a policy with the bank regarding this but it was not the latest revision available provided by the bank . As a result of a comment made by the auditor during the audit, the Town has updated our banking agreement with the Town's financial institution to include the latest revision available.
2. In order to prevent any malware intrusions, etc. the Town will consider providing for a dedicated computer for all online banking activities.
3. The Town will consider a method to insure that bank accounts are monitored for unauthorized or suspicious activity by someone other than the Supervisor's Confidential Clerk. The Board currently reviews all transactions made with status of the bank accounts on a monthly basis via the Supervisor's monthly report.
4. The Town Board will consider a method for the Board to be made aware of the general framework involved for computerized data processing and the general framework for the security of sensitive data when it is processed, stored on backup or transferred electronically.
5. The Town Board will consider a method to educate the Board on the general framework of how the Supervisor's Confidential Clerk manages the Town's electronic information, with the needs and expectations of the Town considered along with the parameters of the level of service. The Town currently receives superior service from the Supervisor's Confidential Clerk but the entire Board could become better aware of what this involves.
6. The Town will consider adopting Information Technology policies and procedures for data security and Information Technology Disaster Recovery.

Respectfully submitted,

Dana Haff – Town of Hartford Supervisor

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

The objective of our audit was to examine the IT controls over the Town's electronic data. To achieve our audit objective and obtain valid evidence, we performed the following procedures:

- We interviewed Town officials and the Clerk to obtain an understanding of the Town's IT operations.

- We inquired about policies and procedures related to security, disaster recovery plans, breach notification and online banking.

- For our sample of online banking transactions, we identified all the online payments and transfers for the period January 1, 2015 through July 31, 2016. We judgmentally selected six months of transactions from every third month (March, June, September and December 2015 and March and June 2016) to determine if the online banking transactions were authorized, supported and for a valid Town purpose. We also determined whether internal bank transfers were legitimately made to Town-owned bank accounts.

We conducted this performance audit in accordance with GAGAS. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

APPENDIX 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

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller
Tracey Hitchen Boyd, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

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

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

BUFFALO REGIONAL OFFICE
Jeffrey D. Mazula, 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

GLENS FALLS REGIONAL OFFICE
Jeffrey P. Leonard, 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: Albany, Clinton, Essex, Franklin, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington Counties

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

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE
Tenneh Blamah, 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: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester Counties

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

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

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

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

STATEWIDE AUDITS
Ann C. Singer, Chief Examiner
State Office Building, Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313