Cash Management Technology

Office of the New York
STATE COMPTROLLER
Thomas P. DiNapoli

Local Government and
School Accountability

INFORMATION TECHNOLOGY SERIES

Table of Contents

Cash Management Technology

Technology can make our lives easier and our governments more efficient. For local governments,[1] the use of cash management technologies requires the review of current procedures to ensure that they are authorized under existing laws and that the design of internal controls is appropriate for securely processing transactions electronically. Some of the newer technologies can speed up the recording and depositing of receipts and can help ensure that disbursements are properly recorded, while reducing the cost of processing these transactions. Traditional internal controls, such as written policies and procedures, authorizations, segregation of duties and monitoring, however, are still important considerations when implementing these technologies.[2]

This guide is designed to give the reader an overview of electronic cash management technologies, as well as the internal controls needed to help detect fraud and ensure that all transactions are captured.

This guide is designed to give the reader an overview of electronic cash management technologies, as well as the internal controls needed to help detect fraud and ensure that all transactions are captured. A key concept is that classic internal controls, if well designed, all work well with cash management technologies.

The ideas presented in this publication should not be construed as recommendations or endorsements of services offered by banks or other commercial vendors. The suggestions in this guide are opportunities for you to consider in the management of your financial operations. You will need to tailor these opportunities to fit the requirements and needs of your local government. You should also inquire about the cost of these services and consider requesting competitive quotations or proposals. Before you enter into any contracts for these services, you should consult with your legal counsel.

Who is Responsible?

The establishment of an appropriate internal control system over cash management technology rests with many people in your local government:

- **Governing Board** – For adopting policies and establishing the “tone at the top” regarding internal controls.
- **Management** (Business and finance officials and department heads) – For designing and implementing control procedures, studying potential risks and keeping current with technological advances in their field.
- **Information Technology** (**IT) Department** – For providing a secure computing environment, including network security.
- **All Other Staff** – For following established procedures and contributing to keeping assets and information secure.

Electronic Funds Transfers

Increasingly, local governments are processing financial transactions electronically. Both receipts and disbursements, in accordance with applicable laws, can be processed via electronic funds transfer (EFT) services. EFT refers to moving funds electronically to and from different bank accounts, either between accounts at the same bank or to accounts at separate financial institutions. Before you begin processing electronic transactions (e-transactions), you should have detailed policies and procedures in place regarding online banking and EFT activities.

Before you begin processing electronic transactions (e-transactions), you should have detailed policies and procedures in place regarding online banking and EFT activities.

Policies and Procedures – A basic foundation is a comprehensive policy that outlines online banking activities and EFTs that your organization is authorized to engage in. This policy should include the following, consistent with the statutory and other legal responsibilities of the officers and employees involved:

- What online banking and EFT activities will be used?
- Who is authorized to initiate e-transactions?
- Who will approve e-transactions?
- Who will transmit e-transactions?
- Who will record e-transactions?

Proper segregation of duties is important in almost any business function but is especially critical for electronic transactions. Without proper segregation of duties, you can increase the risk that one person could be in a position to both commit a wrongdoing and conceal it. At least two individuals should be involved in each e-transaction. The authorization and transmitting functions should be segregated and, if possible, the recording function should also be delegated to someone who does not have either approval or transmitting duties.

When using online banking for electronic disbursements, remember that many of the same controls that would be used when manually preparing a check apply. For instance, the official responsible for preparation of the electronic disbursement should not have the authority to audit and approve claims for payment. Payments made using EFT services cannot circumvent laws, regulations or your internal control policies.

Electronic or Wire Transfers – Electronic or wire transfers are transfers of local government funds, usually effective within minutes of being executed.[3] Wire transfers are usually more costly than other electronic methods of making disbursements and are most commonly used for bond payments, investments or other large-dollar settlements. Other types of electronic transfers are used for small-dollar or repetitive transactions, such as federal, State, or local aid/grant payments, because they are less costly but still efficient.

Access to in-house wire transfer software should be controlled and its use should be authorized and monitored frequently due to the ease with which wire transfers can be made.

Some banks offer wire transfer capability in their online banking applications, allowing you to input the required information and initiate, authorize and transmit wire transfers in-house without outside assistance from your depository. Access to in-house wire transfer software should be controlled and its use should be authorized and monitored frequently due to the ease with which wire transfers can be made. Most wire transfers require only routing numbers and bank account numbers for execution. Other options typically available to initiate a wire transfer include phoning the bank and using a password to verbally authorize the transfer, hand delivering a letter of authorization to the bank with the transfer instructions or sending a fax with the authorized signature and password.

There should be strong authorization controls for wire transfers. Individuals should not be able to execute a wire transfer without obtaining authorization from the custodial officer or a deputy. Before your local government opts to disburse funds by wire transfer, the governing board is required to enter into a written agreement[4] with the bank or trust company in which your funds have been deposited. In addition, you should have a callback provision in your wire instructions that requires the bank to call someone (other than the person initiating the transaction) to confirm the appropriateness of the transfer. You can also establish additional controls, such as a policy that does not allow the bank to initiate wire transfers out of the country or to banks other than the Depository Trust Company for bond payments. Remember, a wire transfer is an immediate settlement of funds; it is like a check that is cashed immediately.

Additionally, you should remember that wire transfers do not normally go through the accounts payable transaction cycle and are sometimes not recorded in the accounting system immediately. Wire transfers are often captured manually (after the fact) through the use of journal entries. If you manually enter these transactions, remember that there are higher risks that errors can occur, such as overdrawing bank accounts or recording incorrect information. Your internal control system must include procedures or safeguards for the documentation and reporting of all transfers and disbursements of funds by electronic or wire transfer.[5] In addition, the bank or trust company must provide the officer requesting the transfer written confirmation of the transaction no later than the business day following the day on which the funds were transmitted.

Online Banking Activities

Most banks offer convenient online banking for their customers. Gone are the days of waiting for the monthly bank statement to arrive to see what has happened or calling the bank to see if a check has cleared. You can now access your accounts online and review transaction activity at any time. While there certainly are benefits to online banking, it is important for local governments to be aware of any vulnerabilities in their IT systems used to process these transactions to avoid any fraudulent activity.

Poor controls over online banking increase the risk that a local government may become the victim of cyberfraud and experience financial losses that may not be recoverable.

Benefits – The benefits of online banking include the ability to review account balances and check clearing activity, make transfers between bank accounts, reconcile accounts frequently and closely monitor cash balances for more effective investing. Online banking also allows you the convenience of moving money yourself from higher interest-bearing accounts to your checking accounts to cover payrolls or accounts payable disbursements as necessary. The ease of online banking also may allow you to make better investment decisions because you can monitor your cash flow and cash balances as frequently as you may need.

Vulnerabilities – Local governments are allowed to disburse or transfer funds in their custody by means of electronic or wire transfer.[6] However, because connecting to the Internet is a necessary part of the online banking process, a multitude of vulnerabilities must be recognized and prepared for. Poor controls over online banking increase the risk that a local government may become the victim of cyberfraud and experience financial losses that may not be recoverable.

Fraud involving the exploitation of valid online banking credentials is a significant risk facing any local government that processes financial transactions online. Some of the more popular types of electronic fraud targeting online banking are phishing attacks,[7] malware,[8] and pharming.[9] In a typical scenario, the targeted individual (or group of individuals) receives an email that contains a malicious attachment or directs the recipient to a malicious website. Once the recipient opens the attachment or visits the website, malware containing a key logger is installed on their computer. The key logger collects login information allowing the perpetrator to impersonate the legitimate user or create another user account. Thereafter, fraudulent electronic cash transfers are initiated and directed to bank accounts in the United States or foreign countries.

Despite the security controls used by online banking establishments, there is no absolute way to guarantee the safety of online banking. The tactics used to commit fraud can range dramatically in sophistication and continually evolve over time. Likewise, there is no single control that is most effective against cyberattacks. A best practice for protecting IT systems, information and local government resources is to build successive layers of defense mechanisms, a strategy referred to as defense-in-depth. In addition to successive layers of technology-based defense, internal controls for local governments that conduct online banking should also include non-technical controls such as written policies and recurring information security awareness training for all employees who use computers connected to the Internet and the local government's network.

Best Practices – The Multi-State Information Sharing and Analysis Center (MS-ISAC) has identified some best practices for internal controls over online banking.[10] These contain elements specifically for online banking, as well as several relating to the overall computing environment in which online banking occurs. The lack of any one particular control does not automatically mean that an online banking environment is vulnerable. All the controls have to be assessed in total to determine their significance and evaluated in the context of appropriate mitigating controls. For example, it may not be practical or appropriate for a local government to dedicate a computer for all online banking transactions. However, online banking risks could be reduced to an acceptable level through a combination of other controls, such as those that follow.

All the controls have to be assessed in total to determine their significance and evaluated in the context of appropriate mitigating controls.

Computing environment best practices include:

- Installing antivirus, anti-spyware, and malware and adware protection software and keeping the software current.
- Installing all new software (including operating system) and hardware patches on a timely basis.
- Installing firewalls and intrusion detection and prevention systems and actively monitoring them, especially for unauthorized or suspicious Internet connections.
- Changing the default login names and passwords on routers, firewalls and other network equipment and software.
- Employing advanced authentication techniques for user logins (e.g., two-factor authentication).[11]
- Holding passwords to complexity requirements,[12] not using the login and password for your financial institution on any other website or software, regularly changing passwords and not allowing the computer or web browser to save login names or passwords.
- Using a wired rather than wireless network for financial transactions, whenever possible.

Online banking best practices include:

- Monitoring bank accounts on a timely basis for unauthorized or suspicious activity and reporting any suspicious activity immediately.
- If possible, using a virtual machine on a single dedicated computer with an Internet Protocol (IP) address that is pre-registered with the financial institution.
- Never accessing the bank's website from a public computer or from an unprotected mobile device.
- Setting up and using a non-administrative user account on the computer.
- Checking with your bank about enabling alerts and other security measures that may be available such as blocking wire transfers to other countries and requiring the verification of transactions over certain amounts, possibly through callbacks, emails or text alerts.
- Providing information security awareness training to educate users on safe computing practices, such as being suspicious of emails and text messages purporting to be from their bank or a government agency, avoiding visiting untrusted websites, not following links provided by untrusted sources or opening suspicious email which appears to be from trusted sources.
- Ensuring that users know what the bank's website looks like and what questions are asked to verify their identity.[13]
- Erasing the web browser cache, temporary Internet files, cookies and history after each online banking session so that if the system is compromised, that information will not be on the system to be stolen by an attacker or malware program.
- Typing the bank's website address into the Internet browser's address bar every time because email and search engine links may not be secure.
- Checking that the session is secure before undertaking any online banking.[14]
- Logging out of all banking websites and closing the browser window.[15]
- Turning off or disconnecting the computer from the Internet by unplugging the modem or ethernet/ DSL cable when finished.[16]
- Entering into written agreements with banks that address and control electronic or wire transfers appropriately.

In addition to addressing the risks of online banking through a combination of technical and non-technical controls, local governments should also discuss the risks with their insurance provider. As the number of instances of such things as cyberfraud and identity theft increases, insurers are actively looking for ways to help their clients manage these risks.

Lockboxes

Lockbox services are provided by a bank or trust company via a contract, in which the bank or trust company receives and processes paper-based payments for you. Lockboxes are convenient and not just for larger organizations. Even the smallest local government can benefit from using this type of service. Lockbox services have become a common banking service and most areas typically have multiple banks and companies competing for lockbox accounts.

The lockbox process is convenient, efficient and can help to segregate the collection duties from the billing and reconciliation functions.

Lockbox services may be used for the collection of real property taxes, special assessments and water and sewer rents. This process would usually involve giving a master file, such as a copy of the tax roll, to the collecting agent (bank). The bank would collect the amounts due, record them as received on the master file and deposit the amounts in your bank account.

A lockbox system is designed to:

- Speed up the processing of payments
- Provide timely information to update accounts receivable records
- Speed up the availability of funds and provide faster access to cash
- Eliminate preparation of bank deposit slips and trips to the bank
- Provide segregation of duties
- Provide added reporting capabilities
- Smooth out the work flow and possibly save on overtime or seasonal employee costs during peak collection periods, i.e., tax collection.

The lockbox process is convenient, efficient and can help to segregate the collection duties from the billing and reconciliation functions. Constant monitoring is very important. If you opt to use a lockbox service, you must ensure that the bank or trust company is properly performing those functions in accordance with statutory requirements[17] and that adequate internal controls are in place at the bank or trust company to safeguard sensitive and confidential data, protect the public's assets and provide assurance that transactions are completely and accurately accounted for. For example, you should perform frequent reconciliations to ensure that the master file minus the amounts collected (and deposited) equals the unpaid amounts to date. You should also ensure that the contract you have with the bank or trust company addresses the process details. In addition, the bank or trust company that is depositing your funds should be designated as an official depository of your local government.

Accepting Credit and Debit Cards

Credit and debit card usage is a common and frequent means for many to conduct financial transactions. If your governing board determines that it is in the public's interest to accept payments by credit and debit card, then the decision to accept these type of payments should be formally approved by a resolution of the governing board and documented in the minutes. The guidelines for accepting credit and debit card payments should be detailed in a written policy.

Your local government can enter into an agreement with one or more financing agencies or card issuers for the acceptance of various payments by credit and debit card.[18] The contract between your local government and the financing agency or card issuer must be awarded in compliance with your procurement policies and procedures.[19] There are advantages and disadvantages to accepting credit and debit cards, which you will need to weigh when deciding whether or not to accept them.

Some of the benefits of accepting payments by credit and debit cards include:

- Increased certainty of collection
- Accelerated payments and availability of funds
- Enhanced customer convenience
- Reduced return check processing costs.

Costs Involved – There are usually transaction fees (service costs) and administrative fees (equipment and personnel costs) involved in processing credit and debit card transactions. Often, local governments struggle with justifying the payment of fees to the financing agency or card issuer for the credit and debit card transactions. Your governing board can opt to charge a service fee to the cardholder. The amount of the service fee is limited to the amount of the costs incurred by the local government in connection with the credit and debit charge. You should use a competitive procurement process to secure the lowest fee possible to minimize the financial impact to the citizens and your local government.

There are advantages and disadvantages to accepting credit and debit cards, which you will need to weigh when deciding whether or not to accept them.

There is also a State contract, which is part of a program known as Electronic Value Transfer (EVT),[20] for accepting credit and debit cards. The EVT contract offers centralized service contracts for payment processing and the necessary equipment and software to support these services. Included in the contract are several nationally recognized credit and debit cards. The EVT contract is most likely available to you for accepting credit and debit cards and should be considered when evaluating the costs involved.[21]

Types of Payments to Accept – You should consider whether you want to accept credit and debit card payments for mandatory charges (such as property taxes and sewer rents) and/or for discretionary charges that citizens elect to pay (such as recreation fees). Credit and debit cards may be accepted for the payment of fines, civil penalties, rents, rates, taxes, fees, charges, revenues, financial obligations or other amounts, including penalties, special assessments or interest, owed to the local government.[22] Accepting credit cards for mandatory charges will not necessarily increase the amount of revenue received, but it may speed up the actual receipt of those revenues. On the other hand, accepting them for discretionary charges might facilitate additional collection of such charges.

Accepting credit cards for mandatory charges will not necessarily increase the amount of revenue received, but it may speed up the actual receipt of those revenues.

Whatever decision you make, among other things, you must have a credit and debit card acceptance agreement with your financing agency or card issuer, and you should also have policies and procedures in place to accept and process the credit and debit card payments on-site.

Accepting Payments via Your Municipal Website

Local governments are also authorized to accept payments of penalties, rents, rates, taxes, fees, interest or other charges through their municipal website or the website of a third-party vendor that has contracted with the local government to receive such payments on its behalf.[23] Payments can be accepted via these websites in the "manner and condition" defined by your local government. As such, your local government has the discretion to reasonably determine the manner in which payments will be accepted, such as by credit and debit cards or electronic funds transfer. However, the municipal or third-party vendor website cannot be the sole method of payment.

Cash Transfer Applications – Local governments can use third-party cash transfer applications (e.g., Paypal, Square, Stripe, Venmo) to accept payments. When this type of application is used, internal controls and best practices related to working with third-party vendors, including a service level agreement, should be established whenever possible. Local governments should clearly indicate the name of their account, so residents can confirm payments are sent to the proper recipient. Officials should also establish a policy that prohibits sending unsolicited emails with account information or links to the payment site, as a way to minimize the success of possible phishing attempts.

Cash Donation Applications – Local governments should avoid using crowdsourcing or crowdfunding applications (e.g., Fundly, GoFundMe, IndieGoGo, Kickstarter). These types of applications are commonly used to collect donations and, when used in that context by a local government, would be considered improper in accordance with GML. However, private civic groups, rather than the local government itself, could solicit donations, and the money collected could be accepted by the local government as a gift.[24] Links to donation collections on a crowdfunding page should not be posted on any of the local government's websites or social media.

Local governments providing online payment capabilities are required to comply with certain provisions of the New York State Technology Law and related regulations, and must, at a minimum, authenticate the identity of the sender and ensure the security of the information transmitted. Also, if your local government accepts payments of taxes on a municipal or third-party vendor website, you must provide a confirmation page, which at least includes the transaction date and amount paid, a unique confirmation number and a notice to the taxpayer to print out and retain the confirmation page as a receipt. Online payments may result in increased collections of certain charges, such as real property taxes by individuals who live outside of the area.

Online payments may result in increased collections of certain charges, such as real property taxes by individuals who live outside of the area.

Remote Deposit Capture

Remote deposit capture (RDC) generally is a service that allows you to scan checks that you receive into your computer or cash register and to transmit the scanned images electronically to your depository, causing your account to be credited. The basic requirements for an RDC service include a computer, an Internet connection, a check scanner and a service provider such as your current depository.

To use RDC you simply load checks into your scanner, which takes a picture of each check and reads the check information. The scanned checks are balanced to create a digital deposit. This digital deposit is then transmitted (over a secure Internet connection) to your RDC bank, who accepts the deposit and posts the deposit to your account.

The benefits of using RDC can include:

- Convenience
- Better deposit availability
- Reduced transportation cost and risk of lost checks
- Enhanced cash flow.

There are potential risks in using RDC. Because the checks you receive are not physically transferred to the bank, you may now be responsible for ensuring RDC scanned items are processed only once. These items could easily be scanned or deposited again in error. Also, it is possible that you will become responsible for safeguarding and eventually destroying checks in accordance with legal requirements. You should work closely with your RDC depository and consult legal counsel on how to appropriately address these risks and any additional potential liability. You should have written procedures that specifically address these concerns. Such procedures should include:

The benefits of using RDC can include convenience; better deposit availability; reduced transportation cost and risk of lost checks; and enhanced cash flow.

- How to identify if a check has been scanned
- Where to securely store scanned checks
- How long to hold on to scanned checks before destroying them
- How to properly destroy scanned checks once the requisite timeframe has expired.

Check Images

Many banks have ended the practice of returning original canceled paper checks to their customers. In place of canceled checks, your bank probably has asked you to accept some other record of checks charged to your account. The form of documentation you receive is based on your agreement with your bank. It is important that you set up your service agreement with the bank to receive the information you need for your operations. Most likely you are receiving one of the following:

You can accept these electronic images of your checks in lieu of statutory requirements for canceled checks upon authorization by your governing board.

- **Statements of Check Images** – Statements showing images of the fronts and backs of canceled checks. Normally, each statement will display multiple check images.
- **Electronic Check Image**s – Compact discs (CDs) containing images of the fronts and backs of canceled checks or online access via the Internet to allow viewing (and printing) of the fronts and backs of the canceled checks.

You can accept these electronic images of your checks in lieu of statutory requirements for canceled checks upon authorization by your governing board.[25] Also remember that if the bank provides you with electronic images, the check image must show both sides of the check and should show the magnetic ink character recognition (MICR)[26] line for bank reconciliation and auditing purposes.

Electronic Signatures

It is often unreasonable to expect the chief fiscal officer, treasurer or other custodian of public funds to hand sign each and every check that your local government issues. Even though electronic or facsimile signatures are commonly used today, it is still important that access to these signatures be controlled. We have issued several audit reports[27] that detail how the cash custodian gave up rights to affix his or her signature on checks and exposed the local government to a higher risk of fraud.

Even though electronic or facsimile signatures are commonly used today, it is still important that access to these signatures be controlled.

When either a digital or facsimile signature is authorized by law and is used, it is important that the custodian of the funds (i.e., treasurer or town supervisor) guard his or her signature from unauthorized use at all times.

Weak controls over signature authority increase the risk that unauthorized individuals may disburse funds for improper purposes.

The following are basic controls that could be used to safeguard the signature of the cash custodian.

- If the signature is part of software that generates a signature on checks, the process that affixes the signature should be password protected. That password should only be known by the cash custodian, and he or she should enter it when needed.
- If a third party prepares your checks for disbursement (e.g., a payroll company or a BOCES), the checks should be returned to the cash custodian for the signature process.
- If the signature is affixed by a plate placed in a check signing machine, it should be under the direct control and supervision of the cash custodian at all times. The signature plate should not be handed out freely or be accessible to employees.

Check Fraud Protection Practices

An effective check fraud prevention tool is a “positive pay” system. This type of system is an automated check matching service offered by most banks that compares checks issued with checks presented for payment. The bank compares the account number, check number and dollar amount of checks presented for payment against the list of checks authorized and issued by you. If your depository receives a check that does not match the information in your record, it identifies it as an exception item. You should instruct your depository to return all nonconforming items (exceptions) as the default procedure. This will give you an opportunity to review unmatched checks within the return item timeframe specified by your depository. Ensure that a clear policy exists to segregate staff approving “positive pay” exceptions and staff initially preparing the checks.

It is also a good idea to maintain tight check security – store checks, check reorder forms, canceled checks (or check images) and signature plates under lock and key.

For those governments with a relatively small check volume, a “reverse positive pay” system could be considered instead. This service provides you with a daily checks paid information report that can be matched against your internal check issue file. You would download the list of paid checks from the bank and compare them to your list of issued and authorized checks.

Both services allow you to make payment/no payment decisions and can help protect you against possible check fraud. However, neither service is foolproof, nor will a bank give you a warranty against all check fraud losses.

It is also a good idea to maintain tight check security – store checks, check reorder forms, canceled checks (or check images) and signature plates under lock and key. Restrict employee and cleaning crew access, examine new checks when they arrive, keep check boxes sealed until needed and maintain a check log/inventory.

Conclusion

As new electronic technologies continue to emerge in the commercial sector, they will certainly migrate to government as well. Our laws and our internal controls will need to adapt and embrace these new technologies as they will provide opportunities for increased efficiency and cost reductions in the processing of financial transactions, as well as new opportunities for fraud.

We encourage local officials to consider the cash management technologies discussed in this guide when they are appropriate for the size and complexity of their operations. Before implementing any of these technologies, the governing board should be provided with objective information regarding the risks, costs and benefits of these services. Legal counsel should review all agreements with service providers to ensure that your rights and assets are adequately protected.

We encourage local officials to consider the cash management technologies discussed in this guide when they are appropriate for the size and complexity of their operations.

The Office of the State Comptroller would be pleased to assist you with any questions you may have regarding the information contained in this guide. The addresses and telephone numbers of our regional offices are located at the end of this publication.

Resources

- *Information Technology Governance* Local Government Management Guide
  https://www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf
- *Ransomware* Local Government Management Guide
  https://www.osc.ny.gov/files/local-government/publications/pdf/ransomware.pdf

New York State Office of General Services

- State Contracts
  https://ogs.ny.gov/procurement/ogs-centralized-contracts-list
- Electronic Value Transfer Administrator
  https://ogs.ny.gov/procurement/electronic-value-transfer-evt-services-contracts

New York State Chief Information Security Office (CISO)

- **https://its.ny.gov/ciso/local-government**

Notes

[1] In this guide, the term "local governments" generally refers to all municipal corporations (counties, cities, towns and villages), school districts and boards of cooperative educational services (BOCES), district corporations (e.g., fire districts), special improvement districts governed by a separate board of commissioners and public libraries.

[2] See *The Practice of Internal Controls* Local Government Management Guide for additional internal control considerations at **www.osc.ny.gov/files/local-government/publications/pdf/practiceinternalcontrols.pdf**

[3] New York State General Municipal Law (GML), Section 5-a, authorizes officers to disburse or transfer funds in their custody by means of electronic or wire transfer.

[4] The written agreement must indicate the manner in which electronic or wire transfers will be made, identify by name and number those accounts from which electronic or wire transfers may be made, identify which officer(s) is authorized to order an electronic or wire transfer of funds and implement a security procedure as defined in Uniform Commercial Code, Section 4-A-201. This latter requirement includes a procedure established by agreement with the bank for the purpose of verifying that a payment order is that of the local government and detecting errors in transmission or the content of the payment order.

[5] GML, Section 5-a

[6] GML, Section 5-a

[7] Phishing attacks use fake email messages or other techniques, sometimes pretending to represent a bank, to trick you into providing personal or financial information. The email requests information such as name, password and account number and provides links to a fake website.

[8] Malware is malicious software (i.e., ransomware, viruses, Trojans, spyware, rootkits and worms) that typically is installed without the user's knowledge or consent. Such software is specifically designed to harm computer systems and electronic data, often by deleting files, gathering sensitive information or making systems inoperable. The different types of malware can capture keystrokes for login information, monitor and capture other data to authenticate identity, generate web pages that appear to be legitimate and hijack a browser to transfer funds without the user's knowledge.

[9] Pharming involves the installation of malicious code on a computer and can take place without any conscious actions on the part of the user. For example, a user opens an email or email attachment that installs malicious code and later redirects the user to a fake website that closely resembles the user's bank site. Information provided while on the fake website is visible to an attacker.

[10] See the MS-ISAC Security Primer – *Online Banking Safety*, issued March 2017 **www.cisecurity.org/wp-content/uploads/2017/03/Security-Primer-Online-Banking.pdf**.

[11] Typically, two-factor authentication is a sign-on process where a person proves their identity with two of the three methods: something you know (e.g., username and password or PIN), something you have (e.g., smartcard or token) or something you are (e.g., fingerprint or iris scan).

[12] Passwords should contain an uppercase character, a lowercase character, a numeric character and a special character (e.g., %, #, @) and should not include the use of names or words that can be easily guessed or identified using a password-cracking mechanism. They should also be at least eight characters in length.

[13] A vigilant user can sometimes spot a fake bank website by noticing slight modifications to the bank's standard page – for example, extra security questions, bad grammar, misspellings, a fuzzy or older logo or a change in the location of each feature.

Notes

[14] Users should check whether the website accessed for online banking starts with https:// instead of http://. The "s" indicates a secure connection. The connection uses the secure sockets layer (SSL) protocol to encrypt data between the user's computer and the bank's server.

[15] It is important to log off completely from Internet banking websites. Simply closing the browser window or tab used to perform the transaction may not close the banking session. If the computer became infected or compromised, the user's session could be taken over by an attacker or malware program and then used to perform unauthorized financial transactions without the user's knowledge.

[16] Shutting down the computer when it is not in use can limit exposure to malware. Contrary to popular belief, not all cyberfrauds require the user to take an action such as opening a malicious email attachment or visiting a malicious website.

[17] Real Property Tax Law, Section 996; GML, Section 99-t

[18] Pursuant to the authority in GML, Section 5

[19] GML, Section 104-b

[20] The New York State Office of General Services is the State's EVT administrator. More information on this program can be found at: **https://ogs.ny.gov/procurement/electronic-value-transfer-evt-services-contracts**.

[21] To the extent authorized by law (such as GML, Sections 5 and 5-b), local governments and school districts may use this State contract.

[22] GML, Section 5

[23] GML, Section 5-b

[24] See Opinions of the New York State Comptroller, Nos. 1978-256 and 1980-768.

[25] GML, Section 99-b[2]

[26] A MICR line contains information that can be useful during the audit process such as the bank routing number, bank account number, check number, check amount and other information printed near the bottom of the check in magnetic ink. Examination of the MICR line can disclose errors that occurred during the check-cashing process or possible irregularities.

[27] Examples include: Madison County (2019M-142), Patchogue-Medford Public Library (2019M-126), Town of Benson (2019M-54) and Cortland County (2018M-247). OSC audit reports can be found on our website: **https://www.osc.ny.gov/local-government/audits.**

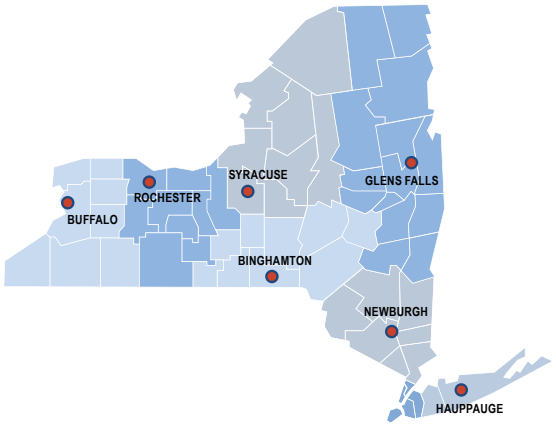
Contacts

New York State Comptroller
THOMAS P. DiNAPOLI

Division of Local Government and School Accountability

110 State Street, 12th Floor, Albany, NY 12236
Tel: 518.474.4037 • Fax: 518.486.6479
Email: localgov@osc.ny.gov

www.osc.ny.gov/local-government



Andrea C. Miller
Executive Deputy Comptroller

Executive • 518.474.4037
Robin L. Lois, CPA, Deputy Comptroller
Simonia Brown, Assistant Comptroller
Randy Partridge, Assistant Comptroller

Audits, Local Government Services and Professional Standards • 518.474.5404
(Audits, Technical Assistance, Accounting and Audit Standards)

Local Government and School Accountability Help Line • 866.321.8503 or 518.408.4934
(Electronic Filing, Financial Reporting, Justice Courts, Training)

Division of Legal Services
Municipal Law Section • 518.474.5586

New York State & Local Retirement System
Retirement Information Services
Inquiries on Employee Benefits and Programs
518.474.7736

Technical Assistance is available at any of our Regional Offices

BINGHAMTON REGIONAL OFFICE
Tel 607.721.8306 • **Fax** 607.721.8313 • **Email** Muni-Binghamton@osc.ny.gov
Counties: Broome, Chemung, Chenango, Cortland, Delaware, Otsego, Schoharie, Tioga, Tompkins

BUFFALO REGIONAL OFFICE
Tel 716.847.3647 • **Fax** 716.847.3643 • **Email** Muni-Buffalo@osc.ny.gov
Counties: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming

GLENS FALLS REGIONAL OFFICE
Tel 518.793.0057 • **Fax** 518.793.5797 • **Email** Muni-GlensFalls@osc.ny.gov
Counties: Albany, Clinton, Columbia, Essex, Franklin, Fulton, Greene, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington

HAUPPAUGE REGIONAL OFFICE
Tel 631.952.6534 • **Fax** 631.952.6530 • **Email** Muni-Hauppauge@osc.ny.gov
Counties: Nassau, Suffolk

NEWBURGH REGIONAL OFFICE
Tel 845.567.0858 • **Fax** 845.567.0080 • **Email** Muni-Newburgh@osc.ny.gov
Counties: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester

ROCHESTER REGIONAL OFFICE
Tel 585.454.2460 • **Fax** 585.454.3545 • **Email** Muni-Rochester@osc.ny.gov
Counties: Cayuga, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates

SYRACUSE REGIONAL OFFICE
Tel 315.428.4192 • **Fax** 315.426.2119 • **Email** Muni-Syracuse@osc.ny.gov
Counties: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence

STATEWIDE AUDIT
Tel 607.721.8306 • **Fax** 607.721.8313 • **Email** Muni-Statewide@osc.ny.gov

osc.ny.gov

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability

110 State Street, 12th floor
Albany, NY 12236
Tel: (518) 474-4037
Fax: (518) 486-6479
or email us: localgov@osc.ny.gov

www.osc.ny.gov/local-government

Updated December 2021