Office of the New York State Comptroller

Division of Local Government and School Accountability

LOCAL GOVERNMENT MANAGEMENT GUIDE

Cash Management Technology

Thomas P. DiNapoli State Comptroller

For additional copies of this report contact:

Division of
Local Government and School Accountability
110 State Street, 12th floor
Albany, New York 12236
Tel: (518) 474- 4037
Fax: (518) 486- 6479
or email us:
localgov@osc.state.ny.us

www.osc.state.ny.us **May 2010**

Table of Contents

Cash Management Technology

Technology can make our lives easier and our governments more efficient. For local governments, 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.

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 the new cash 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 or school district. 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.

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.

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

Who is Responsible for Internal Controls Over Cash Technology?

- **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.
- **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 and school districts 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. 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
- Who will review and reconcile e-transactions and how often.

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 electronic 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, the same controls generally apply as would be used when manually preparing a check. 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 or school district funds, usually effective within minutes of being executed.[1] Wire transfers are usually more costly than other electronic methods of making disbursements, and are therefore 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.

Some banks offer wire transfer capability in their online banking applications, which allows 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.

Wire transfers are usually more costly than other electronic methods of making disbursements, and are therefore most commonly used for bond payments, investments, or other large-dollar settlements.

[1] General Municipal Law, Section 5-a, authorizes officers to disburse or transfer funds in their custody by means of electronic or wire transfer.

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.

There should be strong authorization controls for wire transfers. A cash manager or other individual should not be able to execute a wire transfer without obtaining authorization from the custodial officer or a deputy. Before your organization opts to disburse funds by wire transfer, the governing board is required to enter into a written agreement[2] 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 (DTC) 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.[3] 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.

[2] 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.

[3] General Municipal Law, Section 5-a

Online Banking Activities

Most banks offer some type of 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 information technology systems used to process these transactions to avoid any fraudulent activity.

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 only when absolutely 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[4] in their custody by means of electronic or wire transfer. 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.

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.

[4] General Municipal Law, Section 5-a

A best practice for protecting information technology systems, information, and local government resources is to build successive layers of defense mechanisms, a strategy referred to as defense-in-depth.

There has been a significant increase in fraud involving the exploitation of valid online banking credentials. Some of the more popular types of electronic fraud targeting online banking that have emerged are phishing attacks,[5] malware,[6] and pharming.[7] In a typical scenario, the targeted entity receives an email, which either contains an infected attachment, or directs the recipient to an infected website. Once the recipient opens the attachment or visits the website, malware containing a key logger is installed on their computer. The key logger harvests login information allowing the perpetrator to masquerade as 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 cyber attacks. A best practice for protecting information technology 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.

[5] Phishing attacks use fake email messages pretending to represent a bank. The email requests information such as name, password and account number and provides links to a fake website.

[6] Malware is malicious software (i.e., viruses, Trojans, spyware, rootkits, and worms) that typically is installed without the user's knowledge or consent. Such software 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.

[7] 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.

Best Practices - A well-respected consortium of State and federal agencies has identified some best practices for internal controls over online banking.[8] They 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 insecure. All the controls have to be assessed in total to determine their significance and evaluated in the context of appropriate mitigating controls. For example, a local government may not be able to afford a dedicated computer to be used for all online banking transactions. However, they may be able to reduce online banking risks to an acceptable level through a combination of other controls.

Computing Environment Best Practices include:

- Installing antivirus, anti-spyware, and malware and adware detection software and keeping the software current through recurring, automatic updates
- Installing all new software (including operating system) and hardware patches on a timely basis
- Installing firewalls and intrusion detection and prevention systems and monitoring them on a timely basis, especially for unauthorized/ suspicious Internet connections coming to and leaving the network. IP addresses from foreign countries can also be blocked using access control lists in conjunction with a firewall.
- Changing the default login names and passwords on routers, firewalls and other network equipment and software
- Employing advanced authentication techniques for user logins (i.e., two-factor authentication)[9]
- Holding passwords to complexity requirements,[10] 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.

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.

[8] Cyber Security Advisory issued March 8, 2010 – *Information and Recommendations Regarding Unauthorized Wire Transfers Relating to Compromised Cyber Networks*; **http://www.cscic.state.ny.us/documents/Wire-transfer-fraud-recommendations-2010.pdf.**

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

[10] 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.

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.

Online Banking Best Practices include:

- Monitoring bank accounts on a timely basis for unauthorized or suspicious activity and reporting any suspicious activity immediately
- Using a dedicated computer for online banking transactions, one that is not used for email or Internet browsing
- 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
- 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, and avoiding visiting un-trusted websites, following links provided by un-trusted sources and opening suspicious email which appear 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[11]
- Erasing the web browser cache, temporary Internet files, cookies, and history so that if the system is compromised, that information will not be on the system to be stolen by a hacker or malware program
- Typing the bank's website address into the Internet browser's address bar every time; since email and search engine links are not secure
- Checking that the session is secure before undertaking any online banking[12]
- Logging out of all banking websites and closing the browser window[13]
- Turning off or disconnecting the computer from the Internet by unplugging the modem or Ethernet/DSL cable when finished[14]
- 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 cyber fraud and identity theft increases, insurers are actively looking for ways to help their clients manage these risks.

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

[12] Users should check whether the website accessed for online banking starts with https:// instead of http://. The "s" indicates a secure transaction. The transaction uses the Secure Sockets Layer (SSL) protocol, which enables the encryption of data between the user's computer and the bank's server through public key authentication.

[13] It is important to completely log off from Internet banking sessions. Simply closing the window in which the transaction was performed may not close the banking session. If the computer became infected with a banking Trojan, the user's session could be hijacked and financial transactions could be performed without the user's knowledge.

[14] Shutting down the computer when it is not in use can limit exposure to worms/Trojans that exploit vulnerabilities in operating systems. Contrary to popular belief, not all cyberfrauds require the user to have taken an action such as opening emails or visiting malicious websites.

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 or school district 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.

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,[15] 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 that is depositing your funds should be designated as an official depository of your local government or school district.

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

[15] Real Property Tax Law, Section 996; General Municipal Law, Section 99-t

Accepting Credit/Debit Cards

If your governing board determines that it is in the public's interest to accept payments by credit/debit card, then the decision to accept these type of payments should be formally approved by a resolution of the governing body and documented in the minutes.

Credit/debit card usage is a common and frequent means for many of us to conduct financial transactions. The ability to use credit/debit cards to pay for services is not nearly as widespread in government as it is in the private sector but use is growing. If your governing board determines that it is in the public's interest to accept payments by credit/debit card, then the decision to accept these type of payments should be formally approved by a resolution of the governing body and documented in the minutes. The guidelines for accepting credit/debit card payments should be detailed in a written policy such as your credit/debit card policy.

Your local government or school district can enter into an agreement with one or more financing agencies or card issuers for the acceptance of various payments by credit/debit card.[16] The contract between your local government or school district and the financing agency or card issuer must be awarded in compliance with your procurement policies and procedures.[17] There are of course advantages and disadvantages to accepting credit/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/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/debit card transactions. Often, local governments struggle with justifying the payment of fees to the financing agency or card issuer for the credit/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 or school district in connection with the credit/debit charge. You should use a competitive procurement process to secure the lowest fee possible to minimize the financial impact to the consumer and your local government or school district.

[16] Pursuant to the authority in General Municipal Law, Section 5

[17] General Municipal Law, Section 104-b

There is also a State contract, which is part of a program known as Electronic Value Transfer (EVT),[18] for accepting credit/debit cards. The EVT contract offers centralized service contracts for financial 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/debit cards and should be considered when evaluating the costs involved.[19]

Types of Payments to Accept – You should consider whether you want to accept credit/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/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 or school district.[20] 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.

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

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.

[18] The Department of Taxation and Finance is the State's EVT administrator. More information on this contract can be found on the Department of Taxation and Finance's website at: **www.tax.state.ny.us/evta/overview.htm.**

[19] To the extent authorized by law (such as General Municipal Law, Sections 5 and 5-b), local governments and school districts may utilize this State contract.

[20] General Municipal Law, Section 5

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 your municipal website.

Local governments are also authorized to accept payments of penalties, rents, rates, taxes, fees, interest or other charges through your municipal website.[21] Payments can be accepted via the municipal website 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/debit card or electronic funds transfer. However, the municipal website cannot be the sole method of payment.

Local governments providing online payment capabilities are required to comply with certain provisions of the 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 website, you must provide a confirmation page, which at least includes the transaction date 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 payment of real property taxes by individuals who live outside of the area.

[21] General Municipal Law, Section 5-b

Remote Deposit Capture

Remote deposit capture (RDC) generally is a service which 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, reads the check information, and detects missing required 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, which then accepts the deposit and posts the deposit to your account.

The benefits of using remote deposit capture can include:

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

There are potential risks in using RDC. Since 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:

- 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.

Remote deposit capture (RDC) generally is a service which 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.

Check Images

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

Many banks have ended the practice of returning original cancelled paper checks to their customers. In place of cancelled 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:

- **Statements of Check Images** – statements showing images of the fronts and backs of cancelled checks. Normally, each statement will display multiple check images.
- **Electronic Check Images** – banks sometimes provide compact discs (CDs) containing images of the fronts and backs of cancelled checks or provide online access via the Internet to allow viewing (and printing) of the fronts and backs of the cancelled checks.

You can accept these electronic images of your checks in lieu of statutory requirements for cancelled checks upon authorization by your governing board.[22] 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)[23] line for bank reconciliation and auditing purposes.

[22] General Municipal Law, Section 99-b[2]

[23] A MICR line contains information that can be useful during the audit process such as the bank routing number, bank account number, check number, the 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.

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 organization 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[24] that detail how the cash custodian gave up rights to affix his or her signature on checks and exposed the organization to a higher risk of fraud.

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 (i.e., 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.

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

[24] Examples include: Canandaigua City School District (2009M-148), Cato-Meridan Central School District (2009M-193), and Falconer Central School District (2009M-14). All OSC audit reports can be found on our website: **http://osc.state.ny.us/localgov/audits.**

Check Fraud Protection Practices

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

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. 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.

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, cancelled checks (or check images), and signature plates under lock and key. Restrict employee and cleaning crew access. Examine new checks when they arrive and keep check boxes sealed until needed.

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.

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.

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.

Resources

Electronic Value Transfer Administrator (NYS Department of Tax and Finance)
http://www.tax.state.ny.us/evta/default.htm

Office of General Services State Contracts
http://www.ogs.state.ny.us/purchase/searchbrowse.asp

Government Finance Officers Association (GFOA) Recommended Practices
http://www.gfoa.org/index.php?option=com_content&task=view&id=118&Itemid=130

New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC)
http://www.cscic.state.ny.us/localgov

Division of Local Government and School Accountability

Central Office Directory

Andrew A. SanFilippo, Executive Deputy Comptroller

(Area code for the following is 518 unless otherwise specified)

Executive 474-4037
Gabriel F. Deyo, Deputy Comptroller
Nathaalie N. Carey, Assistant Comptroller

Audits, Local Government Services and Professional Standards 474-5404
(Audits, Technical Assistance, Accounting and Audit Standards)

Local Government and School Accountability Help Line ..... (866)321-8503 or 408-4934
(Electronic Filing, Financial Reporting, Justice Courts, Training)

New York State Retirement System

Retirement Information Services

Inquiries on Employee Benefits and Programs 474-7736

Bureau of Member and Employer Services ..... (866)805-0990 or 474-1101

Monthly Reporting Inquiries 474-1080
Audits and Plan Changes 474-0167
All Other Employer Inquiries 474-6535

Division of Legal Services

Municipal Law Section 474-5586

Other OSC Offices

Bureau of State Expenditures 486-3017

Bureau of State Contracts 474-4622

Mailing Address for all of the above:

Office of the State Comptroller,
110 State St., Albany, New York 12236
email: **localgov@osc.state.ny.us**

Division of Local Government and School Accountability

Regional Office Directory

Andrew A. SanFilippo, Executive Deputy Comptroller

Gabriel F. Deyo, Deputy Comptroller (518) 474-4037

Nathaalie N. Carey, Assistant Comptroller

Cole H. Hickland, Director • **Jack Dougherty**, Director
Direct Services (518) 474-5480

BINGHAMTON REGIONAL OFFICE - H. Todd Eames, Chief Examiner
State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417
Tel (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
295 Main Street, Suite 1032 • Buffalo, New York 14203-2510
Tel (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
One Broad Street Plaza • Glens Falls, New York 12801-4396
Tel (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
NYS Office Building, Room 3A10 • 250 Veterans Memorial Highway • Hauppauge, New York 11788-5533
Tel (631) 952-6534 • **Fax** (631) 952-6530 • **Email:** Muni-Hauppauge@osc.state.ny.us
Serving: Nassau, Suffolk counties

NEWBURGH REGIONAL OFFICE – Tenneh Blamah, Chief Examiner
33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725
Tel (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
The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608
Tel (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
State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428
Tel (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 AUDIT - Ann C. Singer, Chief Examiner
State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417
Tel (607) 721-8306 • **Fax** (607) 721-8313

New York State
Office of the State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor • Albany, New York 12236