

# Bank Account Fraud Protection

The original recommended practice was developed by the Government Finance Officers Association (GFOA). Some aspects of the practice have been revised by the Financial Management Capacity Building Committee (FMCBC) for use by Nova Scotia municipal governments. The original GFOA recommended practice was *Cheque Fraud Protection and Use of Positive Pay*, but has been combined to the current *Bank Account Fraud Protection*, and approved by the GFOA in 2007. Other sources used are footnoted in the text.

## Recommendation

The GFOA recommends that municipalities should establish measures against different types of bank account fraud. Municipalities need to ensure that they develop internal controls and steps to protect themselves.

## Purpose

Municipalities need to take measures to ensure that they are protecting themselves and their customers. Municipalities should develop internal controls and policies for the different types of payment methods they offer. Fraud protection for both cheque payments and automatic payments through bank accounts need to be addressed. Cheque fraud is still a very real problem that is too often overlooked. A cheque that falls into the wrong hands can be altered and cashed. Given the large volume of cheques passing through a municipality, a fraudulent cheque may be paid.<sup>1</sup> Furthermore, as paying municipal bills and taxes through automated banking and direct online banking, bank accounts have become more common targets for fraud and theft. As a result, municipalities should enlist internal controls and security measures.

## Background

Advances in technology have forced both public and private sectors to increase security measures to prevent theft and fraud. Although cheques are not the predominant form of payment in local governments, cheque fraud has increased due to technology. Because of technology, automated banking and online banking have become more popular. Because these methods are new, they may not have the proper control measures to protect the municipality and ratepayers from fraud.<sup>2</sup>

---

<sup>1</sup> Ombudsman for Banking Services and Investments. [Annual Report 1999](http://www.obsi.ca/images/up-OMB_Rprt_99_English.pdf).  
[http://www.obsi.ca/images/up-OMB\\_Rprt\\_99\\_English.pdf](http://www.obsi.ca/images/up-OMB_Rprt_99_English.pdf).

<sup>2</sup> Statistics Canada. [A Feasibility Report on Improving the Measurement of Fraud in Canada](http://dsp-psd.tpsgc.gc.ca/Collection/Statcan/85-569-X/85-569-XIE2006001.pdf). 2005.  
<http://dsp-psd.tpsgc.gc.ca/Collection/Statcan/85-569-X/85-569-XIE2006001.pdf>.

## Considerations for Policy Development

In order for municipalities to develop effective cheque and bank account fraud protection measures, various internal control measures and procedures should be developed. Different internal control measures and procedures will need to be taken for both cheque fraud and bank account fraud. Because cheque fraud and bank account fraud are quite different, the two types have been developed separately. *Appendix I* outlines internal controls, security features, banking services, and procedures that should be considered when developing cheque fraud protection measures.

In addition to developing internal controls and procedures for cheque fraud, municipalities should also consider acquiring positive pay services. Positive pay is one of the most effective services offered against cheque fraud. Many businesses and different levels of government use positive pay to prevent cheque fraud. For more information on the benefits of positive pay, see *Appendix II*.

In addition to cheque fraud prevention and positive pay, municipalities need to develop proper protections against bank account fraud. *Appendix III* illustrates the internal controls and procedures that should be in place surrounding bank account payments.

## Appendices

Appendix I: Internal Controls and Procedures to Prevent Cheque Fraud

Appendix II: Positive Pay Services

Appendix III: Bank Account Internal Controls and Measures

## Appendix I: Internal Controls and Procedures to Prevent Cheque Fraud

Municipalities should have a series of fixed internal controls and procedures surrounding cheque handling. This Appendix will describe the core internal controls and security features that municipalities should have with cheque fraud protection. Also, municipalities need to go a step further with more sophisticated and technologically advanced security measures to keep abreast with fraudulent technical advancements. Municipalities can also use their bank to help prevent cheque fraud by utilizing some of their services.

It is important for municipalities to use a combination of all of these measures, because they are not entirely effective alone. For instance, a municipality should not rely on a bank alone to detect any errors, omissions, or fraudulent activities because if certain frauds are not caught within in 24 hours, the bank will not likely compensate the municipality for any of the lost funds.

### *Standard Internal Controls and Security Features*

The following is a list of personnel related internal controls and technically oriented security features. These should all be part of how a municipality prevents cheque fraud.

- Verifying new hires and training all personnel who disburse funds. Training should include a comprehensive review of legal and regulatory guidelines for disbursing funds, as well as the various approaches to detecting common fraud schemes used to steal money.
  - When hiring new individuals, the municipality should subject all applications to:
    - Criminal record check;
    - Credit bureau check;
    - Prior employment; and
    - Education.
  - All applicants should sign a waiver indicating that they will not request access to the results of these tests if they are not successfully hired.
- Follow clear signature review procedures before cheques are mailed.
  - Municipalities should establish a policy clearly outlining the signing authority of an appointed Council and staff members. Cheques should also be signed by at least two people (one elected and one staff member).
  - The policy should include the value of the cheques requiring specific signatures. For instance, the higher the value of the cheque, the less people authorized to sign the cheque. For example: Any cheques issued below \$10,000 should be signed by the Executive Assistant, Treasurer, Chief Administrative Officer, Appointed Council Member, and Mayor. Any cheques issued above \$10,000 should only be signed by the Chief Administrative Officer, Appointed Council Member, and Mayor.

- Centralize disbursement rather than returning issued cheques to individual departments for mailing.
- Take precautions against staff altering payee names on cheques, such as sending outgoing cheques to be mailed later in the day to limit employee access.
- Bank balances should be monitored daily.
- Actual cheques should be reconciled monthly to the bank statement.
- Technical security features should include:
  - Magnetic Ink Character Recognition (MICR) printed text (simulates a solid line that is difficult to reproduce);
  - Toner retention (difficult to change numbers and letters);
  - Watermarks that cannot be removed or easily replaced;
  - Void pantograph, where ‘void’ shows up on photocopied cheques;
  - Thermo graphic ink (changes colour when rubbed); and
  - Fluorescent fibres (shows up under fluorescent lights).<sup>3</sup>
  - Secure cheques
  - Municipalities should develop controls to determine who have access and signing authority to cheques.
  - Only authorized staff should have access to cheque stock, facsimile signature stamps, and cheque order forms.
  - Enforce security features
    - Control of cheque stock should be maintained throughout the entire cheque printing, signing, and dispatch process.
    - The municipality’s cheque stock should be audited regularly.
  - Implement security features on cheque paper stock
    - For example, micro printed text or toner retention.<sup>4</sup>
  - For the proper implementation of cheque technologies, municipalities should consult the Canadian Payments Association (CPA), which offers rules and standards for processing cheques and cheque technology. Information on the CPA can be found at:  
<http://www.cdnpay.ca/home/home.asp>
- Municipalities should select an insurance company that will cover their losses if cheque fraud or theft occurs.

#### *Additional Services Offered by Banks*

The most common cheque fraud prevention service offered by banks is positive pay, however, there are other services that can be effective. The following is a description of two other services offered by most banks, account reconciliation features and cheque imaging.

---

<sup>3</sup> Government Finance Officers Association of Alberta. *Alberta GFOA Newsletter*. November 2003.  
<http://www.gfoa.ab.ca/Newsletter/2003-3rdQuarterNovember.doc>.

<sup>4</sup> Ibid.

#### Account Reconciliation Features

- Most account reconciliation services offer extra protection, such as implementing a maximum dollar control. The bank may automatically return all cheques presented over a pre-determined dollar amount.
- If an internal policy requires multiple or specific signers for all cheques over a certain dollar amount, the bank could furnish on-line images of these cheques for your review and disposition.
- Some banks may offer a stale date feature, which can prevent old cheques (e.g. six months old) from posting to your account. Alternatively, the municipality can ask the bank to provide an online image of stale items to make a pay or return decision on each one.<sup>5</sup>

#### Cheque Imaging

- Cheque imaging stores the front and back images of paid cheques with access made available to the municipality.
- Cheque imaging (cheque truncation) implementation will be a mandatory banking practice in 2008.
- Finding paid cheques is made easy, and the cheque imaging systems allows users to sort to access.<sup>6</sup>

---

<sup>5</sup> Government Finance Officers Association of Alberta. Alberta GFOA Newsletter. November 2003. <http://www.gfoa.ab.ca/Newsletter/2003-3rdQuarterNovember.doc>.

<sup>6</sup> RBC Centura: Information Reporting Services. WebACCESS – Internet-based Information Reporting and Funds Transfer Service. <http://www.rbccentura.com/business/cashman/inforeport.html>.

## Appendix II: Positive Pay Services

In addition to internal controls and procedures, municipalities should consider including positive pay among its cheque fraud prevention measures. Positive pay is a service offered by most banks in Canada and the United States, and is used by many levels of governments, and public and private sector businesses. It is arguably the most efficient and effective mechanism to prevent or detect cheque fraud. Positive pay is a service that helps to identify fraudulently issued or altered cheques.<sup>7</sup> The following is a description of the general positive pay process:

- A comparison is performed based on cheque serial number and amount between cheques being cleared through the bank;<sup>8</sup>
- The bank requires that an electronic file be sent to the bank for each cheque run that outlines the details of cheques to be issued, including payee details;
- Incoming cheques are monitored and unmatched items, including altered payee, are flagged for immediate action; and
- On a daily basis, the bank advises the municipality of any exceptions.<sup>9</sup>

In addition to checking the serial numbers to determine if the cheques are fraudulent, there are other benefits to using positive pay. The following is a list of some benefits of positive pay.

- Improved cash controls by enabling more timely and accurate reporting, regardless of the size of the municipality.
- May reduce municipal administration associated with fraudulent cheques.<sup>10</sup>
- By alerting a municipality to exception items quickly, the risk of honouring fraudulent items is reduced.<sup>11</sup>
- Positive pay systems streamline the management process with online access to exception records and images of used cheques, and the ability to immediately make pay/no pay decisions online.<sup>12</sup>

Positive pay services are likely already offered by a municipality's current bank. If not, positive pay services are quite common, and should be easy to solicit.<sup>13</sup>

---

<sup>7</sup> HSBC. Positive Pay. <http://www.hsbc.ca/1/2/en/business/cash-management/liquidity-and-accounts-management/positive-pay>.

<sup>8</sup> Ibid.

<sup>9</sup> Government Finance Officers Association of Alberta. Alberta GFOA Newsletter. November 2003. <http://www.gfoa.ab.ca/Newsletter/2003-3rdQuarterNovember.doc>.

<sup>10</sup> HSBC. Positive Pay. <http://www.hsbc.ca/1/2/en/business/cash-management/liquidity-and-accounts-management/positive-pay>.

<sup>11</sup> Bank of Montreal Capital Markets. Positive Pay. <http://www.bmocm.com/products/treasury/cashmanagement/managepay/pp/default.aspx>.

<sup>12</sup> Ibid.

<sup>13</sup> Positive pay may not be available at all small bank branches in municipalities. Municipalities may need to seek a larger centre or head branch for positive pay services.

*Reverse Positive Pay*

Although positive pay is regarded as very successful for protecting municipalities against cheque fraud, some municipalities may be interested in the less costly service of reverse positive pay. Reverse positive pay assists in detecting potential cheque fraud, but the difference it reverse positive pay allows municipalities to conduct its own daily matching procedures. Reserve positive pay places more responsibility and onus with the municipality instead of the bank. Most banks will offer a daily transmission of paid items that can be compared with the municipality's issued cheque file. The municipality must research each suspicious document and advise the bank of items to be returned.<sup>14</sup> This method places more control with the municipality and less control with the bank.

---

<sup>14</sup> Draves, Joe and Toni Nelson. "Check Fraud Risks". Municipal Research and Services Center for Washington. March 2006. <http://www.mrsc.org/focus/finadvisor/fina0306.aspx>.

## Appendix III: Bank Account Internal Controls and Measures

As online banking and paying bills online becomes more popular, municipalities will have to take measures to protect themselves and ratepayers from fraud and theft. Since these methods of payment are relatively new, many municipal governments have not adopted significant security measures. As a result, the GFOA has compiled a list of recommendations for municipalities to include in their internal control measures against bank account theft and fraud.

### 1. Include internal controls and policies that protect all bank accounts from identification from outside sources.<sup>15</sup>

Municipalities should include controls that protect ratepayer's account information from fraud and theft. The following are some measures that should be included in a municipality's internal controls policy:

- Verify new hires and training all personnel who will work with the bank account information. Training should include a comprehensive review of legal and regulatory guidelines for confidentiality, as well as the various approaches to detecting common fraud schemes used to steal money.
  - When hiring new individuals, the municipality should subject all applications to:
    - Criminal record check;
    - Credit bureau check;
    - Prior employment; and
    - Education.
  - All applicants should sign a waiver indicating that they will not request access to the results of these tests if they are not successfully hired.
- Ensure the bank account information remains confidential.
  - Limit the number of employees able to access the information.
  - Apply strict rules and separation of duties to ensure that the confidential information cannot be used for fraud or theft.
- Ensure that the ratepayer's information is given through a secure server.
  - Transactions should be completed using a browser with at least 128 bit encryption.<sup>16</sup>
  - The information should remain encrypted until processed by the municipality. Payments should also be processed regularly and as frequently as possible to ensure the information does not 'sit' anywhere for very long. By allowing the information to 'sit', it could become susceptible to fraud or theft through computer hackers.<sup>17</sup>

---

<sup>15</sup> Government Finance Officers Association. Bank Account Fraud March 2007.

<http://www.gfoa.org/downloads/cashbankaccountfraud.pdf>.

<sup>16</sup> The City of Calgary. Security Our Commitment to Your Privacy.

<sup>17</sup> The City of Calgary. Additional Security Information.

[http://www.calgary.ca/portal/server.pt/gateway/PTARGS\\_0\\_2\\_104\\_0\\_0\\_35/http://content.calgary.ca/CCA/City+Hall/Business+Units/Recreation/Registration/Additional+Security+Information.htm](http://www.calgary.ca/portal/server.pt/gateway/PTARGS_0_2_104_0_0_35/http://content.calgary.ca/CCA/City+Hall/Business+Units/Recreation/Registration/Additional+Security+Information.htm)

**2. Segregation of duties for payments and transactions.**

Municipalities should establish proper segregation of duties to prevent internal fraud. Different employees should be responsible for payments and transactions. There should always be a supervisor or additional person overseeing payments and transactions to ensure that only required payments and transactions are being made. Furthermore, there should be frequent changes in duties and positions to prevent employees from conducting fraud and theft.

**3. Place total blocks on automated banking accounts that are not disbursement accounts.<sup>18</sup>**

If a ratepayer wants to pay the municipality through direct deposit or online banking, the ratepayer should only be able to make payments, and not receive funds transferred from the municipality. If a municipality owes a ratepayer any amount of funds, it should be credited to their account, or they should be issued a cheque.

**4. Place selective blocks on automated banking disbursement accounts.<sup>19</sup>**

In a municipality's bank account protection policy, they should reserve the ability to block a ratepayer's account. If a situation arises where the ratepayer's bank account continually has non-sufficient funds, the account should be blocked and the municipality should begin procedures for removing the service.

**5. Develop a formal plan to review blocks placed on accounts. At a minimum, this should be done on an annual basis.<sup>20</sup>**

---

<sup>18</sup> Government Finance Officers Association. Bank Account Fraud March 2007.  
<http://www.gfoa.org/downloads/cashbankaccountfraud.pdf>.

<sup>19</sup> Ibid.

<sup>20</sup> Ibid.

## References

- Bank of Montreal Capital Markets. Positive Pay.  
<http://www.bmocm.com/products/treasury/cashmanagement/managepay/pp/default.aspx>.
- California Municipal Treasurers Association. Dollars & Sense. Winter 2003.  
[http://www.cmta.org/newsletter/03\\_Winter\\_Newsletter.pdf](http://www.cmta.org/newsletter/03_Winter_Newsletter.pdf).
- Canadian Banking Ombudsman Inc. Annual Report 1999.  
[http://www.obsi.ca/obsi/pages\\_english/includes/xcontent/annrep\\_archive/99.pdf](http://www.obsi.ca/obsi/pages_english/includes/xcontent/annrep_archive/99.pdf).
- Draves, Joe and Toni Nelson. “Check Fraud Risks”. Municipal Research and Services Center for Washington. March 2006.  
<http://www.mrsc.org/focus/finadvisor/fina0306.aspx>.
- Government Finance Officers Association of Alberta. Alberta GFOA Newsletter. November 2003.  
<http://www.gfoa.ab.ca/Newsletter/2003-3rdQuarterNovember.doc>.
- Government Finance Officers Association. Bank Account Fraud Approved, 2007.  
<http://www.gfoa.org/downloads/cashbankaccountfraud.pdf>.
- HSBC. Positive Pay. <http://www.hsbc.ca/1/2/en/business/cash-management/liquidity-and-accountsmanagement/positive-pay>.
- RBC Centura: Information Reporting Services. WebACCESS – Internet-based Information Reporting and Funds Transfer Service.  
<http://www.rbccentura.com/business/cashman/inforeport.html>.
- Statistics Canada. A Feasibility Report on Improving the Measurement of Fraud in Canada. 2005.  
<http://dsp-psd.tpsgc.gc.ca/Collection/Statcan/85-569-X/85-569-XIE2006001.pdf>.
- The City of Calgary. Security Our Commitment to Your Privacy.
- The City of Calgary. Additional Security Information.  
[http://www.calgary.ca/portal/server.pt/gateway/PTARGS\\_0\\_2\\_104\\_0\\_0\\_35/http://content.calgary.ca/CCA/City+Hall/Business+Units/Recreation/Registration/Additional+Security+Information.htm](http://www.calgary.ca/portal/server.pt/gateway/PTARGS_0_2_104_0_0_35/http://content.calgary.ca/CCA/City+Hall/Business+Units/Recreation/Registration/Additional+Security+Information.htm).