RESOLUTION R-26-09

A RESOLUTION ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM POLICY

WHEREAS, the Fair and Accurate Credit Transactions Act of 2003, an amendment to the Fair Credit Reporting Act, required rules regarding identity theft protection to be promulgated; and

WHEREAS, those rules become effective May 1, 2009, and require municipal utilities and other departments to implement an identity theft program and policy; and

WHEREAS, the City of Wheaton has determined that the following policy is in the best interest of the municipality and its citizens.

NOW, THEREFORE, BE IT RESOLVED by the Mayor and City Council of the City of Wheaton, Illinois, that the identity theft prevention program policy dated April 15, 2009 is hereby adopted.

ADOPTED this 20th day of April, 2009.

Mayor

ATTEST:

City Clerk

Roll Call Vote

Ayes:	Councilman Prendiville Councilman Suess Councilman Johnson Councilman Levine Mayor Gresk Councilman Mouhelis
Nays:	None
Absent:	Councilwoman Corry

Motion Carried Unanimously

R-26-09

CITY OF WHEATON
IDENTITY THEFT PROGRAM AND PREVENTION POLICY

The following Identity Theft Program and Prevention Policy (the "Policy") is to implement the requirements of the Fair and Accurate Credit Transactions Act of 2003 and the associated final "Red Flag" rules promulgated by the Federal Trade Commission requiring certain municipal utilities and departments to enact certain policies and procedures regarding Identity Theft Red Flags and Prevention.

SECTION 1: BACKGROUND

The risk to the City, its employees and customers from data loss and identity theft is of significant concern to the City and can be reduced only through the combined efforts of every employee and contractor.

SECTION 2: PURPOSE

A. The City adopts this Policy to help protect employees, customers, contractors and the City from damages related to the loss or misuse of sensitive information. This Policy will:

1. Define sensitive information.
2. Place the City in compliance with state and federal law regarding identity theft protection.

B. This policy enables the City to protect existing customers, reduce risk from identity fraud, and minimize potential damage to the City from fraudulent new accounts. The Policy will help the City:

1. Identify risks that signify potentially fraudulent activity within new or existing covered accounts.
2. Detect risks when they occur in covered accounts.
3. Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed.
4. Update the Policy periodically, including reviewing the accounts that are covered and the identified risks that are part of the Policy.

SECTION 3: SCOPE

This Policy applies to employees, contractors, consultants, temporary workers, and other workers at the City, including all personnel affiliated with third parties.

SECTION 4: SENSITIVE INFORMATION POLICY

A. Definition of Sensitive Information: Sensitive Information includes the following items whether stored in electronic or printed format which could be used on its own or in conjunction with other information to commit identity theft:

1. Credit card information, including any of the following:
   a. Credit card number (in part or whole)
   b. Credit card expiration date
   c. Cardholder name
   d. Cardholder address

2. Other personal information belonging to any customer, employee or contractor, examples of which include:
   a. Names
   b. Address
   c. Phone numbers
   d. Date of Birth
   e. Customer account number

B. City personnel are expected to use the utmost of care in securing Sensitive Information. Furthermore, this section should be read in conjunction with the Illinois Public Records Act, the City's information technology policies and guidelines and the City's local records policy. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor.

SECTION 5: IDENTITY THEFT PREVENTION PROGRAM

A. Definition of a Covered Account: Any customer account that involves or is designed to permit multiple payments or transactions. Every new and existing customer account that meets the following criteria is a Covered Account and is covered by this Policy:
   1. Business, personal and household accounts for which there is a reasonably foreseeable risk of identity theft; or
   2. Business, personal and household accounts for which there is a reasonably foreseeable risk to the safety or soundness of the City from identity theft, including financial, operational, compliance, reputation, or litigation risks.

B. Definition of a Red Flag: Any potential indicators of fraud. Any time a Red Flag, or a situation closely resembling a Red Flag, is apparent, it should be investigated for verification. Examples of Red Flags include:
   1. Alerts, notifications or warnings from a consumer reporting agency or service provider.
   2. Suspicious documents, such as:
      a. Documents provided for identification that appear to have been altered or forged.
      b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
      c. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
      d. Other information on the identification is not consistent with readily accessible information that is on file with the City.
      e. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
   3. Suspicious personal identifying information, such as:
      a. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the City. For example, the address on an application is the same as the address provided on a fraudulent application.
      b. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the City. For example:
         (i) The address on an application is fictitious, a mail drop, or a prison.
         (ii) The phone number is invalid or is associated with a pager or answering service.

c. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other customers or other persons opening accounts.
d. The customer or the person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
e. Personal identifying information provided is not consistent with personal identifying information that is on file with the City.

4. Unusual use of, or suspicious activity related to, a Covered Account, such as:
   a. A new utility account is used in a manner commonly associated with known patterns of fraud patterns. For example, the customer fails to make the first payment or makes an initial payment but no subsequent payments.
   b. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
      (i) Nonpayment when there is no history of late or missed payments.
      (ii) A material change in purchasing or usage patterns.
   c. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
   d. The City is notified that the customer is not receiving paper account statements.
   e. The City is notified of unauthorized charges or transactions in connection with a customer's covered account.
   f. The City receives notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the City.
   g. The City is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

SECTION 6: RESPONDING TO RED FLAGS

A. Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the City from damages and loss.

B. Once potentially fraudulent activity is detected, the employee should gather all related documentation and write a description of the situation. This information should be presented to the designated authority for review, assessment and determination.

C. The designated authority will complete additional investigation and authentication to determine whether the attempted transaction was fraudulent or authentic.

D. If a transaction is determined to be fraudulent or an attempt at fraud, appropriate actions should be promptly taken including:
   1. Continue to monitor an account for evidence of Identity Theft
   2. Contact the customer
   3. Not open a new account
   4. Close an existing account
   5. Reopen an account with a new number
   6. Notify and cooperate with appropriate law enforcement
   7. Determine that no response is warranted under the particular circumstances

SECTION 7: PERIODIC UPDATES TO POLICY

A. This Policy will be reviewed and updated to reflect changes in risk to customers and the soundness of the City from identity theft. If warranted, the Finance Department will update the Policy or present the City Council and City Manager's Office with recommended changes and the City Council or City Manager will make a determination of whether to accept, modify or reject those changes to the Program.

B. Periodic reviews will include an assessment of which accounts are covered by the Policy and whether there are any new accounts.

C. As part of the review, Red Flags may be revised, replaced or eliminated. Defining new Red Flags may also be appropriate.

D. Actions to take in the event that fraudulent activity is discovered may also require revision to reduce potential damages or losses to the City and its customers.

SECTION 8: POLICY ADMINISTRATION

A. Involvement of Management
1. This Policy shall be a separate program and operation and shall not be operated as an extension to existing fraud prevention programs, and its importance warrants the highest level of attention.
2. Implementation of the Policy is the responsibility of the corporate authorities of the City and approval of the initial policy is to be appropriately documented and maintained.
3. Operational responsibility for the Policy is delegated to the Director of Finance.

B. Staff Training
1. Staff training shall be conducted for all employees for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to the City or its customers.
2. The Director of Finance is responsible for ensuring identity theft training for all requisite employees.
3. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the Policy are made.

C. Oversight of Service Provider Arrangements
1. It is the responsibility of the City to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
2. The City will require, by contract, that service providers have such policies and procedures in place.
3. The City will require, by contract, that service providers read, understand and agree to the guidelines set forth in the City's Identity Theft Program and Prevention Policy and report any Red Flags to the Program Administrator.
4. Any specific requirements should be specifically addressed in the appropriate contract arrangements.