CITY OF APPLETON POLICY	TITLE: **IDENTITY THEFT PREVENTION POLICY**		
ISSUE DATE: **March 2009**	LAST UPDATE:	SECTION: Finance	FILE NAME: Red Flag Policy 2008.doc
POLICY SOURCE: Finance Department			TOTAL PAGES: 3
Reviewed by Attorney's Office Date: February 2009	Administrative Services Committee Approval Date: March 11, 2009		Council Approval Date: March 18, 2009

I. Purpose

To establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003

II. Policy

In accordance with Federal Trade Commission regulations, the City establishes an Identity Theft Prevention policy related to the opening and maintaining of covered accounts which will identify, detect, and respond to patterns, practices or specific activities known as "red flags".

III. Definitions

A. **Identity Theft** Fraud committed or attempted using the identifying information of another person.

B. **Red Flag** A pattern, practice or specific activity that indicates the possible existence of identity theft.

C. **Covered Accounts**

1. An account that the City offers or maintains, primarily for personal, family or household purposes that permits multiple payments or transactions. Covered accounts related to City operations include refuse service and utility accounts and deferred special assessment arrangements.
2. Any other account that the City offers or maintains for which there is a reasonably foreseeable risk to customers, or to the safety and soundness of the City from identity theft.

IV. Procedures

A “red flag” is a pattern, practice, or specific activity that indicates the possible existence of identity theft. In order to detect, prevent and mitigate these activities, the City of Appleton establishes an identity theft prevention program which includes reasonable policies and procedures to:

A. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the Program.
B. Detect red flags that have been incorporated into the Program.
C. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft
D. Ensure the Program is updated periodically to reflect changes in risk to customers and to the safety and soundness of the City from identity theft.

V. Identification of Relevant Red Flags

In order to identify relevant red flags, the City considered the types of accounts it offers and maintains, the methods it provides to open these accounts, the methods it provides to access these accounts, and its previous experience with identity theft. Based on this consideration, the City identified relevant red flags from the following:

A. The presentation of suspicious documents. This would include: documents that appear to be forged or altered; documents on which a person’s photograph or physical description is not consistent with the person presenting the documentation; or, receiving documentation with information that is not consistent with existing customer information.
B. The presentation of suspicious personal identifying information. This would include: a customer’s address or phone number being the same as that of another customer; a customer failing to provide complete personal identifying information on an application when reminded to do so; or, a customer’s identifying information not being consistent with the information that may be on file for the customer.
C. The unusual use of, or other suspicious activity related to, a covered account. This would include: mail being sent to an account holder that is repeatedly returned undeliverable; receiving notice that a customer is not receiving his or her paper statements; or, a customer’s account being used in a way that is not consistent with the customer’s history (such as late or no payments when the account has been timely in the past).
D. Notice from customers, victims of identity theft, law enforcement authorities, or persons regarding possible identity theft in connection with covered accounts.

VI. Detection of Red Flags

In order to detect any of the red flags identified above, the City will:
A. Record change of address requests for existing accounts.
B. Require sensitive data changes (i.e. ACH banking information) of existing accounts be completed in writing and signed by the customer.
C. Require sensitive data (i.e. ACH banking information) be submitted in writing for

the opening of accounts and signed by the customer.
D. Monitor customer transaction history for unusual trends or transactions.

VII. Response

Any employee that may suspect fraud or detect a red flag will implement one or more of the following responses as applicable in order to prevent and mitigate identity theft. The response shall be commensurate with the degree of risk posed.

A. Continue to monitor the account for evidence of identity theft.
B. Contact the customer for additional information or documentation.
C. Reopen an account with a new account number.
D. Not open a new account.
E. Close an existing account.
F. Change any passwords, security codes or other security devices that permit access to the account.
G. Notify law enforcement.
H. Determine no response is warranted under the particular circumstances.

VIII. Updating the Program

The program shall be updated periodically to reflect changes in risks to customers or to the safety and soundness of the City from identity theft. The following factors will be taken into consideration in determining the necessity for updating the program.

A. The experiences of the City with identity theft.
B. Changes in methods of identity theft.
C. Changes in methods to detect, prevent and mitigate identity theft.
D. Changes in the types of accounts that the City offers or maintains.
E. Changes in the business arrangements of the City.

IV. Administration of Program

A. The Director of Finance, or designee, shall be responsible for the development, implementation, oversight and continued administration of the Program.
B. Staff training shall be conducted for all employees, officials and contractors 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.
C. In the event the City engages a service provider to perform an activity in connection with one or more accounts, the Finance Director, or designee, shall ensure that all activities are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, will be considered to be meeting these requirements.