Standard Administrative Policy and Procedures Manual

Title: **FINANCIAL POLICY**	Date of Version: **MAY 17, 2010**
Section: **IDENTITY THEFT PREVENTION POLICY**	Resolution No.: **2010-114**

SECTION 1 - PURPOSE

The purpose of this policy is to establish an Identity Theft Prevention Program ("Program") designed to detect, prevent and mitigate identity theft in connection with the opening and maintenance of a covered account and to provide continued administration of the Program in compliance with the Federal Trade Commission's ("FTC") Red Flag Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003, 16 C. F. R. § 681.2.

SECTION 2 – DEFINITIONS

Account means a continuing relationship established by a person with the City to obtain services for personal, family, household or business purposes and includes an extension of credit, such as the purchase of services involving a deferred payment.

Covered account means:

A. An account the City offers or maintains primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions. Covered accounts include utility billing and ambulance billing accounts; and

B. Any other account 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, including financial, operational, compliance, reputation or litigation risks.

Identity theft means fraud committed or attempted using the identifying information of another person without authority.

Identifying information means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:

A. Name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

B. Medicare number;

C. Member identification number; or

D. Claim number

Red Flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

SECTION 3 - PROGRAM

The City establishes an Identity Theft Prevention Program to detect, prevent and mitigate identity theft. The Program shall include 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; and

D. Ensure the Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the customers form identity theft.

SECTION 4 - IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the City considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with identity theft. The City identifies the following Red Flags, in each of the listed categories:

A. Notifications and Warnings from Consumer Reporting Agencies or Local Law Enforcement

1. Notice or report from a consumer reporting agency;

2. Report of fraud from a consumer reporting agency or local law enforcement; and

3. Indication from a consumer report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the documentation;
3. Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

1. Identifying information presented that is inconsistent with other sources of information;
2. Identifying information presented that is inconsistent with other information the customer provides (such as inconsistent birth dates);
3. Identifying information presented that is the same as shown on other applications found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious mailing address);
5. Social security number presented is the same as one given by another customer;
6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security number must not be required); and
8. A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

1. Change of address for an account followed by a request to change the account holder's name;
2. Account used in a way that is not consistent with prior use (such as late or no payments when the account has been timely in the past);

3. Mail sent to the account holder is repeatedly returned as undeliverable;

4. Notice to the City that a customer is not receiving mail sent by the City;

5. Notice to the City that an account has unauthorized activity;

6. Breach in the City's computer system security; or

7. Unauthorized access to or use of customer account information.

E. Alerts from Others

1. Notice to the City from a customer, an identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

<u>SECTION 5</u> - DETECTION OF RED FLAGS

A. New Accounts

In order to detect any of the Red Flags identified above with the opening of a new account, City personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require a completed application form;

2. Require certain identifying information such as name, date of birth, residential or business address, driver's license or other identification;

3. Verify the customer's identity by reviewing a driver's license or other identification card.

4. Independently contact the customer, if necessary.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing account, the City personnel will take the following steps to monitor transactions with an account:

1. Verify the identification of customers if they request information, whether in person, via telephone, via facsimile or e-mail;

2. Verify the validity of requests to change billing addresses; and

3. Verify changes in banking information given for billing and payment purposes.

SECTION 6 – MITIGATING AND PREVENTING IDENTITY THEFT

In the event City personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red flag:

A. Continue to monitor an account for evidence of identity theft;

B. Contact the customer;

C. Change any passwords or other security devices that permit access to accounts.

D. Not open a new account;

E. Close an existing account;

F. Reopen an account with a new account number;

G. Determine that no response is warranted under the particular circumstances;

H. Notify law enforcement; or

I. Notify the program administrator (as defined below) for determination of the appropriate step(s) to take.

In order to further prevent the likelihood of identity theft occurring, the City will take the following steps with respect to its internal operating procedures:

A. Each workstation will make sure the computer monitor is turned so that customers at the counter cannot see private information.

B. All computers are password protected and logged off when not in use.

C. Password-activated screen savers will be used to lock employee computers after a period of inactivity.

D. Passwords will not be shared or posted near workstations.

E. Private information is stored in locked files until the account is inactive for at least one year at which time it will be shredded.

F. Offices are set up so non employees cannot access the computers or trash to obtain information illegally.

G. Private information is kept under lock and key.

H. Only specially identified employees with a legitimate need will have access to the key.

I. Employees maintain a “Clean Desk Policy” which means when the employee is going to be away from the desk paperwork will be removed from the desk or put into a locked file.

<u>SECTION 7</u> - UPDATING THE PROGRAM AND THE RED FLAGS

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the City from identity theft. At least yearly the Program Administrator will consider the City’s experiences with identity theft situation, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the City maintains and changes in the City’s business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will present the City Council with his or her recommended changes and City Council will make a determination of whether to accept, modify or reject those changes to the Program.

<u>SECTION 8</u> - PROGRAM ADMINISTRATION

A. Oversight

The City’s Program will be overseen by a Program Administrator. The Program Administrator shall be the Finance Director. The Program Administrator will be responsible for the Program's administration, for ensuring appropriate training of City staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances, reviewing and, if necessary, approving changes to the Program.

B. Staff Hiring and Training

City staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. Special procedures will be followed when hiring new employees who would have access to the customer accounts.

1. Check references or do background checks before hiring employees who will have access to sensitive data.

2. New employees sign an agreement to follow our confidentiality and security standards for handling sensitive data.

3. Access to customer’s personal identifying information is limited to the employees who need to know.

C. Service Provider Arrangements

In the event the City engages a service provider to perform an activity in connection with one or more accounts, the City will take the steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.