CITY OF ISSAQUAH

Identity Theft Prevention Program

Effective beginning May 1, 2009

I. PROGRAM ADOPTION

The City of Issaquah ("Utility") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flag Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 16 C. F. R. § 681.2. This Program was developed and approved by the City Council. After consideration of the size and complexity of the Utility's operations and account systems, and the nature and scope of the Utility's activities, the City Council determined that this Program was appropriate for the City of Issaquah, and therefore adopted this Program on April 6, 2009.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

Under the Red Flag Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to the size, complexity and nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4. Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from Identity Theft.

B. Red Flags Rule definitions used in this Program

The Red Flag Rule defines "Identity Theft" as "fraud committed using the identifying information of another person" and a "Red Flag" as "a pattern, practice, or specific activity that indicates the possible existence of Identity Theft."

According to the Rule, a municipal utility is a creditor subject to the Rule requirements. The Rule defines creditors "to include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."

All the Utility's accounts that are individual utility service accounts held by customers of the utility whether residential, commercial or industrial are covered by the Rule. Under the Rule, a "covered account" is:

1. Any account the Utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and

2. Any other account the Utility offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Utility from Identity Theft.

"Identifying information" is defined under the Rule as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including: 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, unique electronic identification number, computer's Internet Protocol address, or routing code.

III. IDENTIFICATION OF RED FLAGS.

In order to identify relevant Red Flags, the Utility 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 Utility identifies the following Red Flags and will train appropriate staff to recognize these Red Flags as they are encountered in the ordinary course of Utility business:

A. Alerts, Notifications and Warnings From Credit Reporting Agencies

Red Flags

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on a customer or applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant;
4. Notice or report from a credit agency of an address discrepancy; and
5. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity, such as an unusual increase in the volume of credit inquiries, unusual increase in the number of established credit relationships, or a material change in the use of credit.

B. Suspicious Documents

Red Flags

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 document;
3. Other information on identification document is not consistent with information provided by the person opening a new covered account, by the customer presenting the identification, or with existing customer information on file with the creditor (such as a signature card or recent check); and
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides, for instance, where there is a lack of correlation between the social security number range and the date of birth;
2. Identifying information presented that is inconsistent with external sources of information, for instance, an address does not match a consumer report or a social security number is listed in the Social Security Administration's Death Master File;
3. Identifying information presented is associated with common types of fraudulent activity, such as use of a fictitious billing address or phone number;
4. Identifying information presented that is consistent with known fraudulent activity, such as presentation of an invalid phone number or fictitious billing address used in previous fraudulent activity;
5. Social security number presented that 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 numbers 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

Red Flags

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use (example: very high activity);
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to the Utility that a customer is not receiving mail sent by the Utility;
6. Notice to the Utility that an account has unauthorized activity;
7. Breach in the Utility's computer system security; and
8. Unauthorized access to or use of customer account information.

E. Alerts from Others

Red Flag

1. Notice to the Utility from a customer, 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.

IV. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Utility personnel detect any identified Red Flags, such personnel must contact the Finance Director of the City. The Finance Director will then decide which of the following steps should be taken:

1. Continue to monitor an account for evidence of Identity Theft;
2. Contact the customer;
3. Change any passwords or other security devices that permit access to accounts;
4. Not open a new account;
5. Close an existing account;
6. Reopen an account with a new number;
7. Notify law enforcement; or
8. Determine that no response is warranted under the particular circumstances.

V. PROGRAM UPDATES

The City's Risk Management Officer shall serve as Program Administrator. The Program Administrator will periodically review and update this Program to reflect changes in risks to customers and the soundness of the Utility from Identity Theft. In doing so, the Program Administrator will consider the Utility's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the Utility'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 update the Program or present the City Council with his or her recommended changes and the City Council will make a determination of whether to accept, modify or reject those changes to the Program.

VII. PROGRAM ADMINISTRATION.

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the Program Administrator. The Program Administrator will be responsible for the Program's administration, for ensuring appropriate training of Utility staff, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, for determining which steps of prevention and mitigation should be taken in particular circumstances, and for considering periodic changes to the Program.

B. Staff Training and Reports

Utility 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. Staff should prepare a report at least annually for the Program Administrator, including an evaluation of the effectiveness of the Program with respect to opening accounts, existing covered accounts, service provider arrangements, significant incidents involving identity theft and responses, and recommendations for changes to the Program.

C. Service Provider Arrangements

In the event the Utility engages a service provider to perform an activity in connection with one or more accounts, the Utility will take the following 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.

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review the Utility's Program and report any Red Flags to the Program Administrator.

RESOLUTION NO. 2009-04

A RESOLUTION OF THE ISSAQUAH CITY COUNCIL, ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM PURSUANT TO THE FAIR AND ACCURATE CREDIT TRANSACTION ACT OF 2003.

WHEREAS, the municipal utilities of the City of Issaquah are considered "creditors" under the Fair and Accurate Credit Transaction Act of 2003 (Act);

WHEREAS, the municipal utilities of the City of Issaquah extend "credit" as defined in the Act by deferring payment for services rendered;

WHEREAS, the municipal utilities of the City of Issaquah maintain "covered accounts" as defined in the Act; and

WHEREAS, the City of Issaquah desires to adopt a policy establishing an Identity Theft Prevention Program pursuant to the Act;

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF ISSAQUAH DO RESOLVE AS FOLLOWS:

Section 1. Adoption of the Identity Theft Prevention Program. The City of Issaquah's procedures for identifying, detecting, and responding to identity theft, attached hereto as Attachment A and adopted by this reference as if set forth in full, are hereby adopted for use by the City of Issaquah municipal utilities to the full extent consistent with state law.

PASSED by the City Council this 6th day of April , 2009.

APPROVED:

MAUREEN MCCARRY,
COUNCIL PRESIDENT

APPROVED by the Mayor this 6th day of April, 2009.

AVA FRISINGER, MAYOR

FILED this 6th day of April, 2009.

ATTEST:

CHRISTINE L. EGGERS, CITY CLERK

APPROVED AS TO FORM:

BY: _____
OFFICE OF THE CITY ATTORNEY

Resolution No. 2009-04