City of Ellensburg

Identity Theft Prevention Program

Effective beginning December 1, 2008

Historic Ellensburg WASHINGTON

EFF. DATE: 12/01/08 **FINANCE POLICY #:**

ISSUE DATE: 11/17/08 **TITLE:** Identity Theft Prevention

REFERENCE: Federal Trade **APPROVED BY:** ________________
Commission's Red Flag Rule
Section 114 of the Fair and Accurate Credit Transactions Act of 2003
Resolution No

This policy applies to any account the City offers or maintains that involves multiple payments or transactions

I. PROGRAM ADOPTION

The City of Ellensburg developed this Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flags 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 with oversight and approval of 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 Ellensburg, and therefore approved this Program on the 17th day of November, 2008.

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 its size, complexity and the 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 Flags 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 City'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 City offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. 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.

"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. <u>IDENTIFICATION OF RED FLAGS.</u>

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 Credit Reporting Agencies
<u>Red Flags</u>

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.

B. Suspicious Documents
<u>Red Flags</u>

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 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
<u>Red Flags</u>

1. Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);

3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
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 City that a customer is not receiving mail sent by the City;
6. Notice to the City that an account has unauthorized activity;
7. Breach in the City'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 City 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. DETECTING RED FLAGS.

A. New Accounts

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

Detect

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
2. Verify the customer's identity (for instance, review a driver's license or other identification card);
3. Review documentation showing the existence of a business entity; and
4. Independently contact the customer.

B. Existing Accounts

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

Detect

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Utility 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:

Prevent and Mitigate

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 the Program Administrator for determination of the appropriate step(s) to take;
8. Notify law enforcement; or
9. Determine that no response is warranted under the particular circumstances.

Protect customer identifying information

In order to prevent the likelihood of identity theft occurring with respect to City accounts, the City will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing customer information;
3. Ensure that office computers are password protected and that computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer information;
5. Request social security numbers (if any);
6. Ensure computer virus protection is up to date; and
7. Require and keep only the kinds of customer information that are necessary for City purposes.

VI. PROGRAM UPDATES

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the program to prevent Identity Theft. Annually, 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 update and implement the revised Program.

VII. PROGRAM ADMINISTRATION.

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the Finance Director. The Finance Director will be responsible for the following:

- Administering the program,
- developing procedures to implement the policy,
- ensuring appropriate training of City staff on the Program,
- reviewing 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, and
- considering periodic changes to the Program.

B. Staff Training and Reports

Customer Service 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.

The Customer Services staff shall 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 City's Program and report any Red Flags to the Program Administrator.

D. Specific Program Elements and Confidentiality

For the effectiveness of Identity Theft prevention Programs, the Red Flag Rule envisions a degree of confidentiality regarding the City's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices is to be limited to the Management and those employees who need to know them for purposes of preventing Identity Theft. Because this Program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program's general red flag detection, implementation, and prevention practices are listed in this document.

The identifying information of the City customers with covered accounts shall be kept confidential and shall be exempt from public disclosure to the maximum extent authorized by law, including RCW 42.56.230(4). "Credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers, except when disclosure is expressly required by or governed by other law;"