City of Yakima

Utility Services

Identity Theft Prevention Program

Effective January 23, 2009

Identity Theft Prevention Program

Table of Contents

I. PROGRAM ADOPTION

The City of Yakima Utility Services Division ("Utility Services") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 16 C. F. R. § 681.2. This Program takes into consideration the size and complexity of the Utility Services operations and account systems, and the nature and scope of Utility Services activities, the City Council approved this Program on January 20, 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 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 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

Covered Account A "covered account" means:

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

Creditor "Creditor" has the same meaning as defined in Section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a (d), and includes a person or entity that arranges for the extension, renewal or continuation of credit, including the City.

Customer A "customer" means a person or business entity that has a covered account with the City.

Financial Institution "Financial institution" means a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a "transaction account" belonging to a customer.

Identifying Information "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 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 or unique electronic identification number.

Identity Theft "Identity Theft" means fraud committed using the identifying information of another person.

Red Flag A "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

Service Provider "Service provider" means a person or business entity that provides a service directly to the City relating to or connection with a covered account.

III. IDENTIFICATION OF RED FLAGS.

In order to identify relevant Red Flags, Utility Services considers the types of covered accounts that it offers and maintains, the methods it provides to open its covered accounts, the methods it provides to access its covered accounts, and its previous experiences with Identity Theft. Utility Services identifies the following red flags, in each of the listed categories:

A. 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 an active duty alert for an applicant; and

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 document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and

C. Suspicious Personal Identifying Information

Red Flags

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. An address or phone number presented that is the same as that of another person;
6. 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
7. A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Covered Account Activity or Unusual Use of Covered Account

Red Flags

1. Change of address for an covered account followed by a request to change the covered account holder's name;
2. Mail sent to the covered account holder is repeatedly returned as undeliverable;
3. Notice to the City that a customer is not receiving mail sent by the City;
4. Notice to the City that an covered account has unauthorized activity;
5. Breach in the City's computer system security; and
6. Unauthorized access to or use of customer covered account information.

E. Alerts from Others

Red Flag

1. Notice to the City from a customer, identity theft victim, law enforcement , other utility, 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 Covered Accounts

In order to detect any of the Red Flags identified above associated with the opening of a **new covered account**, Utility personnel will take the following steps to obtain and verify the identity of the person opening the covered 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); and
3. Review documentation showing the existence of a business entity if the covered account is under a business name; and
4. Independently contact the customer if there are concerns with the identifying information.

B. Existing Covered Accounts

In order to detect any of the Red Flags identified above for an **existing covered account**, Utility personnel will take the following steps to monitor transactions with a covered 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 Services 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. Prevent and Mitigate

1. Continue to monitor a covered account for evidence of Identity Theft;
2. Contact the customer;
3. Change any passwords or other security devices that permit access to covered accounts;
4. Not open a new covered account;
5. Close an existing covered account;
6. Reopen a covered 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.

B. Protect customer identifying information

In order to further prevent the likelihood of identity theft occurring with respect to Utility Services covered accounts, Utility Services, working closely with the Information Systems Division, will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure that the Utility Services website is secure or provide clear notice if the Utility Services website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing customer information;
3. Ensure that office computers in the Utility Services area are password protected and that computer screens in the Utility Services area lock after a set period of time;
4. Ensure computer virus protection is up to date; and
5. Require and keep only the kinds of customer information that are necessary for utility purposes.

C. Internal Controls Regarding Identifying Information

1. Information Collected

The following identifying information may be collected by Utility Services:

a. Name
b. Service Address
c. Mailing Address
d. Telephone Number
e. Official State /government issued driver's license or identification number
f. Date of Birth
g. Alien registration number
h. Government passport number

i. Employer or taxpayer identification number

2. Collection Methods

Customer personal identifying information will generally be collected by:

a. Presentation by customer at the office
b. Telephone
c. Internet, email fax, or other electronic means
d. Mail
e. Nob Hill Water
f. Yakima County Assessor
g. Yakima County Credit Service

3. Access to Personal Information

a. File cabinets containing personally identifiable information that are not located in the Utility Services office will be stored in a locked room.
b. The Building Superintendant will control keys to the file cabinet and room, make any copies of the keys, and distribute those keys only to employees with a legitimate need.
c. The list of people who have access to the Utility Services area where files are kept, access to the Utility Services Storage area where files are kept, or access to the Utility Services Billing system will be reviewed.
d. Visitors who must enter areas where sensitive files are kept must be escorted by an authorized employee.
e. No visitor will be given any entry codes or allowed unescorted access the office.

4. General Network Security

a. General network security, and firewalls will be managed by the Information Services Division.

5. Password Management

a. Passwords are not to be shared or posted near workstations.
b. Password-activated screen savers will be used to lock employee computers in the Utility Services after a period of inactivity.

6. Paper Records

a. Paper records that contain personal information will be shredded before being placed into the recycling bin.
b. Paper shredders will be available in the Utility Service Conference room.

VIII. PROGRAM ADMINISTRATION.

A. Oversight

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee. The Committee is headed by a Program Administrator who may be the Utility Services manager or their appointee. Two or more other individuals appointed by the Program Administrator comprise the remainder of the committee membership. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of Utility Services 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 and considering periodic changes to the Program.

B. Program Updates

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 Utility Services 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 Utility Services 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.

C. Staff Training and Reports

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. Additional training will occur on a yearly basis or as new methods of Identity Theft are identified. The Program Administrator shall provide a yearly report to City Council detailing incidents of Identity Theft, Utility Services compliance with the Program, the effectiveness of the Program and any recommended changes.

D. Service Provider Arrangements

In the event Utility Services engages a service provider to perform an activity in connection with one or more covered accounts, Utility Services 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 Utility Services Program and report any Red Flags to the Program Administrator.

E. Specific Program Elements and Confidentiality

The identifying information of 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). For the effectiveness of Identity Theft prevention Programs, the Red Flag Rule envisions a degree of confidentiality regarding the Utility's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices are to be limited to the Identity Theft Committee 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.

F. Special or Unusual Circumstances

The Program Administrator, or his/her designee, may waive any provision of this program when specific circumstances render enforcement of such provision impractical or when, in his/her sole judgment, unusual circumstances so warrant. Such waiver may be conditioned on such terms as the Administrator may determine are appropriate. Any person aggrieved by an action of the Administrator regarding such a waiver may appeal the action to the Director of the Department of Finance and Budget. Any person aggrieved by the director's action regarding such appeal may appeal to the City Manager.