City of Sherwood Oregon

Home of the Tualatin River National Wildlife Refuge

RESOLUTION 2009-004

A RESOLUTION ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, the Federal Trade Commission has set forth guidelines for an Identity Theft Prevention Program pursuant to the Red Flags Rule (16 C.F.R. § 681.2) which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 and the Oregon Consumer Identity Theft Protection Act (ORS 646A.622); and

WHEREAS, the Program is intended to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account; and

WHEREAS, those rules became effective November 1, 2008, and require municipal utilities and other departments to implement an identity theft program and policy; and

WHEREAS, the City of Sherwood has determined that the following policy is in the best interest of the municipality and its citizens.

NOW, THEREFORE, THE CITY OF SHERWOOD RESOLVES AS FOLLOWS:

Section 1. The City of Sherwood hereby establishes an Identity Theft Prevention Program as described and set forth in the attached Exhibit A.

Section 2. This resolution will be effective immediately upon adoption by the City Council.

Duly passed by the City Council this 6th day of January 2009.

Keith S. Mays, Mayor

Attest:

Sylvia Murphy, City Recorder

Exhibit A

City of Sherwood
Identity Theft Prevention Program

I. Purpose

The purpose of this program is to establish an Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule (16 C.F.R. § 681.2), which implements Section 114 of the Fair and Accurate Credit Transactions Act (FACT) of 2003 and the Oregon Consumer Identity Theft Protection Act (OCITPA) (ORS 646A.622). The Program is intended to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account, particularly accounts pertaining to the City of Sherwood, Oregon, utility services (Utility).

The Program shall include reasonable policies and procedures to:

1. Identify relevant "red flags," identified below, 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.

II. Definitions

The definitions provided here are taken from 16 C.F.R. § 681.2 and are:

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

Identifying information: 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, driver's license or government-issued identification number, alien registration number, passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing code.

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

Covered account: (1) any account the Utility offers or maintains primarily for personal, family or household purposes, that involve 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.

III. Administration of Program

1. The utility's governing body shall be responsible for the development, implementation, oversight and continued administration of the Program.
2. The Program shall train staff, as necessary, to effectively implement the Program.
3. The Program shall exercise appropriate and effective oversight of service provider arrangements.

IV. The Program: Identification, Detection, Prevention & Mitigation of Red Flags

A. Identification of Red Flags

The Utility identifies the following red flags in each of the five listed categories:

1. Notifications and Warnings from Credit Reporting Agencies

Red Flags include:

a. Report of fraud accompanying a credit report;
b. Notice of report from a credit agency of a credit freeze on a customer or applicant;
c. Notice or report from a credit agency of an active duty alert for an applicant; and
d. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

2. Suspicious Documents

Red Flags include:

a. Identification document or card that appears to be forged, altered or inauthentic;
b. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
c. Other document with inconsistent information pertaining to the customer (such as discrepancies in signatures); and
d. Application for service that appears to have been altered or forged.

3. Suspicious Personal Identifying Information

Red Flags include:

a. Identifying information presented that is inconsistent with other information the customer provides (e.g. inconsistent birth dates);
b. Identifying presented information that is inconsistent with other sources of information (e.g. address does not match address on credit report);
c. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
d. Identifying information presented that is consistent with fraudulent activity (e.g. invalid phone number or fictitious billing address);
e. Provided social security number is the same as one given by another customer;
f. Provided address or phone number is the same as that of another person;
g. Failure 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
h. A person's identifying information is not consistent with the information that is on file for the customer.

4. Suspicious Account Activity or Unusual Use of Account

Red Flags include:

a. Change of address for an account followed by a request to change the account holder's name;
b. Payments stop on an otherwise consistently up-to-date account;
c. Account used in a manner that is inconsistent with prior use (e.g. very high activity);
d. Mail sent to the account holder is repeatedly returned as undeliverable;
e. Notice to the Utility that a customer is not receiving mail sent by the Utility;
f. Notice to the Utility that an account has unauthorized activity;
g. Breach in the Utility's computer system security; and
h. Unauthorized access to or use of customer account information.

5. Alerts from Others

Red Flags include:

a. 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.

B. Detecting Red Flags

Red Flags may be detected in both new and existing accounts, therefore, Utility personnel will take the following steps:

1. New Accounts

a. Obtain and verify the identity of the person opening the account by requiring 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;
b. Review documentation showing the existence of a business entity; and/or
c. Independently contact the customer.

2. Existing Accounts

a. Verify the identification of customers if they request information whether the request is made in person, via telephone, via facsimile, or via email;;
b. Verify the validity of requests to change billing addresses; and
c. Verify changes in banking information given for payment purposes.

C. Preventing and Mitigating Red Flags

In the event that Utility personnel detect red flags, Utility personnel shall take one or more of the following actions, commensurate with the degree of risk posed by the red flag, to prevent and mitigate identity theft. Appropriate actions may include:

1. Monitor an account for evidence of identity theft;
2. Contact the customer;
3. Change any passwords, security codes or other security devises that permit access to a covered account;
4. Refuse to open a new account;
5. Close an existing account;
6. Reopen an account with a new account 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.

In order to further prevent the likelihood of identity theft occurring with respect to Utility accounts, the Utility will take the following steps internally 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;
4. Keep offices clear of papers containing customer information;
5. Ensure computer virus protection software is up to date;
6. Require and keep only the kinds of customer information that are necessary for utility purposes; and
7. Post notices of this policy in common workspaces to remind employees of this policy.

V. Program Updates

The Program shall be updated periodically to reflect changes in risks to customers or to the safety and soundness of the organization from identity theft based on factors such as:

1. The experiences of the organization with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent and mitigate identity theft;
4. Changes in the types of accounts that the organization offers or maintains; or
5. Major changes in the business arrangements of the organization, such as mergers, acquisitions, alliances, joint ventures and service provider arrangements.

VI. Program Administration

A. Oversight

Oversight of the Program shall include:

1. Assignment of specific responsibility for implementation of the Program;
2. Review of reports prepared by staff regarding compliance; and
3. Approval of material changes to the Program as necessary to address changing risks of identity theft.

Responsibility for developing, implementing, and updating this Program is assigned to the City Manager or their designee, who will act as the Program Administrator.

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. Utility staff will provide reports to the Program Administrator on incidents of identity theft.

Utility managers and supervisors are responsible for being familiar with the Identity Theft Protection Act and this Program. Utility managers and supervisors are also responsible for meeting with their staff to assess current compliance and document appropriate safeguard practices in writing.

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 steps to ensure that the activity is conducted in accordance with this Program.

D. Non-disclosure of Security Information

"Security information" is defined as government data that the disclosure of which would be likely to jeopardize the security of information, possessions, individuals or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury

For the effectiveness of this Program, knowledge about specific red flag identification, detection, mitigation and prevention practices must be limited to the Program Administrator and to those employees with a need to know such information.

Any documents that may have been produced or are produced in order to implement this Program that list or describe such practices or information that contain "security information" are not to be made available to the public. Public disclosure of security information would likely jeopardize the security of information against improper use.

VII. Effective Date

This Program takes effect immediately.