

## **RESOLUTION NO. 1965**

### **A RESOLUTION ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM IN ACCORDANCE WITH THE FEDERAL FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003**

#### **THE TROUTDALE CITY COUNCIL FINDS AS FOLLOWS:**

1. The Federal Trade Commission (FTC) adopted rules concerning the adoption of identity theft prevention programs required by the Fair and Accurate Credit Transactions (FACT) Act of 2003, which took effect on January 1, 2008;
2. The FTC's rules (Red Flags Rule) require creditors, such as City utilities, to establish identity theft prevention programs for covered accounts, including utility accounts;
3. The Red Flags Rule requires identity theft prevention programs to provide for the identification, detection, and response to patterns, practices, or specific activities, known as "red flags," that could indicate identity theft;
4. City staff has evaluated the number and type of accounts covered by FACT, the likelihood of damage from identity theft, the cost and operational burden in tracking "red flags," and appropriate responses in the event an identity theft situation develops;
5. The City Attorney has prepared the attached Identity Theft Prevention Program for the City, which is commensurate with the size and complexity of the City's customer accounts and scope of its activities as a creditor for utilities and Municipal Court obligations; and
6. FACT requires the Identity Theft Prevention Program to be effective no later than November 1, 2008.


#### **NOW, THEREFORE, BE IT RESOLVED BY THE COUNCIL OF THE CITY OF TROUTDALE**

Section 1. The Identity Theft Prevention Program attached to this Resolution is adopted.

Section 2. This Resolution is effective on November 1, 2008.

YEAS: 6  
NAYS: 0  
ABSTAINED: 0

  
\_\_\_\_\_  
Paul Thalhofer, Mayor

  
\_\_\_\_\_  
Date

  
\_\_\_\_\_  
Sarah Skroch, Deputy City Recorder

Adopted: October 28, 2008

# CITY OF TROUTDALE

## Identity Theft Prevention Program

Effective beginning November 1, 2008

## **I. PROGRAM ADOPTION**

The City of Troutdale ("City") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule" or "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 Administrator and City Council. After consideration of the size and complexity of the City's operations and account systems, and the nature and scope of the City's activities, the City Council determined that this Program was appropriate for the City of Troutdale, and therefore approved this Program on October 28, 2008.

## **II. PROGRAM PURPOSE AND DEFINITIONS**

### **A. Fulfilling requirements of the Red Flags Rule**

Under the Red Flags 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 City service accounts held by customers of the City 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. 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. The City identifies the following red flags, in each of the listed categories:

#### **A. Notifications and Warnings From Credit Reporting Agencies**

The City currently does not use credit reporting agencies. However, in the event the City does use a credit reporting agency, the City identifies the following red flags:

##### **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; and
- 4) Indication from a credit report of activity that is inconsistent with a customer’s usual pattern or activity.

#### **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
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 (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. Mail sent to the account holder is repeatedly returned as undeliverable;
4. Breach in the City's computer system security; and
5. 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 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 (note that not all identifying information will be needed for all new accounts);
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**, City 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 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:

### **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. Notify the Finance Director for determination of the appropriate step(s) to take;
7. Verify that all contact via the US Postal Service is made using the correct name, address and postage;
8. Notify law enforcement; or
9. Determine that no response is warranted under the particular circumstances.

### **Protect customer identifying information**

In order to further 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 if customers use website to make payments on accounts;
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 only the last 4 digits of 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**

The Finance Director will periodically review and update this Program to reflect changes in risks to customers and the soundness of the City from Identity Theft. In doing so, the Finance Director will consider the City's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the City's business arrangements with other entities. After considering these factors, the Finance Director will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Finance Director will update the 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 Program 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 and considering periodic changes to the Program. The Finance Director is also responsible for ensuring compliance with the Program.

### **B. Staff Training and Reports**

City staff responsible for implementing the Program shall be trained either by or under the direction of the Finance Director in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. Training should occur at least once a year following the Finance Director's review and changes, if any, to the Program. All employees required to participate in Program training must sign a form acknowledging that they have received the required training.

City staff implementing the Program must provide a written report to the Finance Director of any incidents of Identity Theft and the steps taken pursuant to this Program.

City staff implementing the Program is encouraged to provide written reports of the City's compliance with the Program and the effectiveness of the Program.

### **C. Service Provider Arrangements**

The City engages service providers to perform certain activities in connection with various accounts, such as collections. The City 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 Finance Director.

#### **D. Non-disclosure of Specific Practices**

For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices must be limited to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this Program (excluding this document) that list or describe such specific practices and the information those documents contain are considered "security measures" as defined in ORS 192.501(23) and may be unavailable to the public because disclosure of them would reveal or otherwise identify security measures designed to protect certain information against improper use, that use being to circumvent the City's Identity Theft prevention efforts in order to facilitate the commission of Identity Theft.