

RESOLUTION NO. 2146

A RESOLUTION IMPLEMENTING THE WRITTEN IDENTITY THEFT PREVENTION POLICY CONSISTENT WITH THE FAIR AND ACCURATE CREDIT TRANSACTION (FACT) ACT OF 2003 AND OREGON IDENTITY THEFT PREVENTION ACT (OIPTA).

WHEREAS, the City of Wilsonville strives to protect all personal information that can be used by identity thieves, and;

WHEREAS, adoption of the Identity Theft Prevention Program ("Program") is required by the Federal Trade Commission's Red Flags Rule ("Rule") ,(16 C. F. R. § 681.2), which implements Section 114 of the Fair and Accurate Credit Transactions (FACT) Act of 2003 and ORS 646A.622, the Oregon Consumer Identity Theft Protection Act, (OCITPA), and;

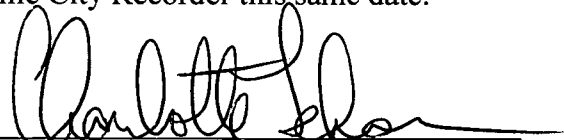
WHEREAS, the policy, as stipulated in the Red Flag Rule, is tailored to the size, complexity and the nature of City's operations, and;

WHEREAS, the policy directs the Finance Director to implement this program that is designed to detect, prevent and mitigate instances of identity theft.

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

1. Hereby adopts the City Identity Theft Protection Policy, attached as Exhibit A.
2. This resolution is effective upon adoption.

ADOPTED by the City Council of the City of Wilsonville at a regular meeting thereof this 20th day of October 2008, and filed with the Wilsonville City Recorder this same date.



CHARLOTTE LEHAN, MAYOR

ATTEST:



Sandra C. King, MMC, City Recorder

SUMMARY of Votes:

Mayor Lehan	Excused
Council President Kirk	Yes
Councilor Knapp	Yes
Councilor Núñez	Yes
Councilor Ripple	Yes

Attachments:

- Exhibit A – Identity Theft Prevention Program
- Staff report

City of Wilsonville

Identity Theft Prevention Program

Effective November 1, 2008

I. PROGRAM ADOPTION

The City of Wilsonville ("City") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), (16 C. F. R. § 681.2), which implements Section 114 of the Fair and Accurate Credit Transactions (FACT) Act of 2003 and ORS 646A.622, the Oregon Consumer Identity Theft Protection Act, (OCITPA). This Program was developed with oversight by the Finance Director ("Program Administrator") and approved by the City of Wilsonville 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 of Wilsonville City Council has determined that this Program was appropriate for the City of Wilsonville, and therefore approved this Program on October 20, 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 utility accounts that are individual utility 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, 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, when used

Red Flags

At the time of adoption, the City does not receive notifications or warnings from any credit reporting agencies. At such time that this becomes a standard business practice, the City shall revise this section appropriately.

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. Verify service address presented to insure that is not 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 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 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. Review documentation showing the existence of a business entity; and/or
3. Independently contact the customer.
4. Customers may be given a seven day grace period between the start of service and the requirement of providing identifying information to the City personnel.

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 extent possible 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 payment purposes.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event City personnel detect 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. Not open a new account;
4. Close an existing account;
5. Reopen an account with a new number;
6. Notify the Program Administrator for determination of the appropriate step(s) to take;
7. Notify law enforcement; or

8. 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;
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 is up to date; and
6. Require and keep only the kinds of customer information that are necessary for City purposes.

VI. PROGRAM UPDATES

The Program Administrator will review and update this Program at least once a year to reflect changes in risks to customers and the soundness of the City from Identity Theft. In doing so, the Program Administrator 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 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 of Wilsonville City Council with his or her recommended changes and the City of Wilsonville 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 an Identity Theft Committee for the City. The Committee is headed by the Program Administrator or his or her appointee. Two or more other individuals appointed by the City Manager for the City of Wilsonville or the Program Administrator comprise the remainder of the committee membership. One of the members should have detailed technical knowledge of the City's computer information systems. The Program Administrator 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.

B. 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. City staff will provide reports to the Program Administrator on incidents of Identity Theft.

Department Heads are responsible to be familiar with the Identity Theft Protection Act and to meet with their staff to assess current compliance and document appropriate safeguard practices in writing.

C. Service Provider Arrangements

In the event the City engages a service provider to perform an activity in connection with one or more accounts, 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 Program Administrator.

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 the Identity Theft Committee who developed this Program and 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 that list or describe such specific practices and the information those documents contain are considered "Security information" (as defined in the following paragraph) and are unavailable to the public because disclosure of them would be likely to substantially jeopardize the security of 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.

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

FINANCE DEPARTMENT STAFF REPORT

Date: October 20, 2008
To: Honorable Mayor and City Council
From: Cathy Alexander, Assistant Finance Director
Subject: Identity Theft Protection Program

SUMMARY:

Adopt the attached Identity Theft Protection Program to fulfill the Federal Trade Commission's Red Flags Rule. This program will also meet the written requirements of the Oregon Consumer Identity Theft Protection Act, (OCITPA).

BACKGROUND:

The City has always maintained the highest level of security possible with our computer and filing systems. Particular attention has always been given to the systems that involve the collection of personal information of our external customers. The Identity Theft Protection Program takes this a step farther as it is designed to provide our employees with the knowledge of what to look for in case of a possible identity theft. These Red Flags will serve as a warning to the employee that further steps may be required to help protect the identity of one of our customers.

The adoption of this program requires an annual review to ensure that the systems we have in place are appropriate and functioning as intended. This review will be made by the Identity Theft committee, which includes the following positions: the Finance Director; the Assistant Finance Director and a representative of the Utility Billing and Municipal Court Clerks.

The program also requires City employees to receive adequate training in Identity Theft Protection. Each new employee will receive a copy of the policy and employees working directly with personal information will be given more in depth training as to what red flags to look for and the proper procedures to be followed in case something suspicious has been found.

RECOMMENDATION:

Staff recommends approval of the Resolution.