

CITY OF WARRENTON

RESOLUTION NO. 2264

RESOLUTION ADOPTING AN IDENTITY THEFT PROGRAM AND PROCEDURES TO COMPLY WITH FEDERAL REGULATIONS AND LAWS RELATING TO UTILITY BILLING

WHEREAS, the Federal Trade Commission has recently promulgated Identity Theft rules requiring the adoption of programs regarding a creditor's detection, prevention, and mitigation of Identity Theft; and

WHEREAS, the Federal Trade Commission's regulations (16 CFR Part 681) specifically apply to governmental utilities which grant "credit" to utility customers through billing for utility services in arrears;

WHEREAS, the Federal Trade Commission's regulations also apply to any City account that the City offers or maintains primarily for personal, family, or household purposes which allows multiple payments or transactions and also to any other City account or program which poses a reasonably foreseeable risk of Identity Theft;

WHEREAS, the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), 15 USC Sections 114 and 315, requires the above-described City accounts or programs to adopt "Red Flag" policies to detect, prevent and mitigate Identity Theft and to protect customers' personally identifiable information; and

WHEREAS, the City of Warrenton provides utility services and bills for such services in arrears, and is therefore subject to the Federal Trade Commission's Red Flag rules and FACT Act; and

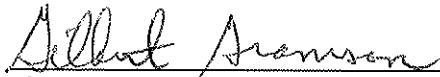
WHEREAS, the City Commission has reviewed the proposed Identity Theft Prevention Program and its own services and accounts and has taken under consideration the degree of risk posed to City customers and accounts, as well as the size and complexity of the City's operations; and

WHEREAS, the City Commission has determined that the Program is appropriate for the City and has approved the Program,

NOW, THEREFORE, BE IT RESOLVED that the Warrenton City Commission hereby adopts the Identity Theft Prevention Program, attached as Exhibit A, incorporated herein, and as may be amended from time to time by the City's Identity Theft Prevention Committee.

PASSED AND ADOPTED BY THE WARRENTON CITY COMMISSION this 28th day of April 2009.

THIS RESOLUTION SHALL BECOME EFFECTIVE ON APRIL 28, 2009.



Gilbert Gramson, Mayor

ATTEST:



Linda Engbretson, City Recorder

RESOLUTION NO. 2264

CITY OF WARRENTON

IDENTITY THEFT PREVENTION PROGRAM

I. Purpose

This policy is intended to establish an Identity Theft Prevention Program (“the Program”). The Program is designed to detect, prevent and mitigate Identity Theft in connection with certain City accounts, programs, or procedures (including specifically utility accounts). This policy applies to City accounts, programs, or procedures which either: 1) allow a person or entity to make multiple payments on personal, family, or household accounts; or 2) present a “reasonably foreseeable risk” of Identity Theft.

As general guidance, this policy will apply to any City account, program, or procedure which allows multiple household or personal payments or collects, transfers, stores, or records a person’s personally identifiable information.

This policy complies with Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act) of 2003 and, by law, is deemed in compliance with the Oregon Identity Theft Act as provided by ORS 646A.622(2)(a) and (b). After consideration of the size and complexity of the City’s operations and the nature and scope of the City’s activities, the City’s governing body has determined that the Program is appropriate for the City and has approved the Program on April 28 2009.

II. Definitions

A covered account means:

1. An account that the City offers or maintains primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions. Covered accounts may include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, *utility accounts*, checking accounts and savings accounts; and
2. Any other account that the City offers or maintains for which there is a reasonably foreseeable risk of Identity Theft to customers or a risk to the safety and soundness of the City’s utility of Identity Theft, including financial, operational, compliance, reputation or litigation risks.

Identify theft means fraud committed or attempted using the Identifying Information of another person without authority.

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

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.

Security Information is defined as government data the disclosure of which would be likely to substantially jeopardize the security of Identifying Information.

III. Program

The City hereby establishes an Identity Theft Prevention Program to detect, prevent and mitigate Identity Theft. The Program includes procedures to:

1. Identify Red Flags for 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 detected Red Flags to prevent and mitigate Identity Theft; and
4. Update the Program periodically to reflect changes in risks to customers and to ensure the safety and soundness of the utility from Identity Theft.

IV. Program Administration

Oversight

Responsibility for developing, implementing and updating this Program lies with the City's Finance Director, who serves as the Program Administrator and the chairperson of the Identity Theft Prevention Committee. The Committee will include five members, the City's Accountant, Utility Billing Clerk, Municipal Court Clerk, Marina Accounting Clerk and the Program Administrator.

The Program Administrator will be responsible for:

1. Program resources and planning;
2. Ensuring appropriate Program training of utility and other affected staff;
3. Reviewing any staff reports regarding Red Flag detection and Identification Theft mitigation and prevention;

4. Determining which steps of prevention and mitigation should be taken in particular circumstances commensurate with the risk posed; and
5. Considering periodic changes to the Program.

The Identity Theft Prevention Committee will be responsible for:

1. Testing for policy compliance;
2. Generating staff reports regarding Red Flag detection and Identification Theft mitigation and prevention;
3. Developing policy revisions for new business processes involving identity information and recommending Program updates; and
4. Reviewing Program activities on a semi-annual basis (or more frequently if necessary).

Staff Training and Reports

Staff responsible for implementing the Program will be trained by or under the direction of the Program Administrator. Staff will provide timely reports to the Program Administrator on all incidents of Identity Theft or occurrences of Red Flags.

Department Heads are responsible for familiarizing themselves with the Program. Department Heads shall meet with their staff annually to assess current compliance.

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 City programs from Identity Theft. In doing so, the Program Administrator will consider the City's experience 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, including the degree of Identity Theft risk posed, the Program Administrator will determine whether changes to the Program, including the listing of new Red Flags, are warranted. If warranted, the Program Administrator will update the Program or present the City's governing body with recommended changes and the governing body will make a determination of whether to accept, modify or reject those changes to the Program.

V. Identification of Red Flags

In order to identify Red Flags, the City considers the types of accounts or programs it offers and maintains, the methods it uses to open and access accounts, and its previous experiences with Identity Theft. The City has identified the following Red Flags in each of the listed categories:

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 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.

Suspicious Documents

Red Flags

1. Identifying Information that appears to be forged, altered or inauthentic;
2. Identifying Information on which a person's photograph or physical description is inconsistent with the person presenting the document;
3. Other document with information that is inconsistent with existing customer information (such as if a person's signature on a check appears forged);
4. Application that appears to have been altered or forged.

Suspicious Personal Identifying Information

Red Flags

1. Identifying Information presented inconsistent with other information the customer provides (example: inconsistent birth dates);
2. Identifying Information presented 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. Failure to provide complete personal Identifying Information on an application when reminded to do so; and
8. Identifying Information inconsistent with the information on file for the customer.

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 inconsistent 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 computer system security; and
8. Unauthorized access to or use of customer account information.

Alerts from Others

Red Flag

1. Notice to the City from a customer, Identity Theft victim, law enforcement or other person that the City has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

VI. Detecting Red Flags

New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new account or program which pertains to household or personal matters (such as a

utility account) or which presents a foreseeable risk of Identity Theft, City personnel may review the below documents to verify the identity of the person or business opening the account. City personnel have the discretion to determine the degree of risk posed and to act accordingly.

1. Required identification may include the following:
 - i. For a U.S. Citizen
 1. Taxpayer Identification number (for business) or Social Security number; and/or
 2. Photo-bearing documents (original required) such as:
 - a. State-issued driver's license; or
 - b. State-issued identification card; or
 - c. Passport from any country
 - ii. For a Non-U.S. Citizen
 1. Social Security number; and/or
 2. Photo-bearing documents (original required) such as:
 - a. State-issued driver's license; or
 - b. State-issued identification card; or
 - c. Passport from any country; or
 - d. Documents containing an alien identification number and country of issuance; or
 - e. Any other photo-bearing government-issued document evidencing nationality or residence.
2. Review all documentation for Red Flags; and/or independently contact the customer.

Existing Accounts

In order to detect any of the Red Flags identified above for an **existing account or program**, personnel will take the below steps to monitor transactions with an account. City personnel have the discretion to determine the degree of risk posed and to act accordingly.

1. Verify customer's Identifying Information if a customer requests any information on the account (this can be done in person, via telephone, via facsimile, or via email);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking information given for payment purposes.

VII. Preventing and Mitigating Identity Theft

1. **Ongoing Operations to Prevent Identity Theft.** In order to further prevent the likelihood of Identity Theft, personnel will take the below steps, commensurate with the degree of risk posed, regarding ongoing internal operating procedures. City personnel have the discretion to determine the degree of risk posed and to act accordingly.

- a. Ensure that its website is secure or provide clear notice that the website is not secure;
- b. Ensure complete and secure destruction of paper documents and computer files containing customer Identifying Information;
- c. Ensure that office computers are password protected;
- d. Keep offices clear of papers containing customer information;
- e. Ensure computer virus protection is up-to-date;
- f. Require and keep only information necessary for your program purposes;
- g. Transmit Identifying Information using only approved methods and include the following statement on any transmitted Identifying Information:

"This message may contain confidential and/or proprietary information, and is intended for the person/entity to which it was originally addressed. If you have received this email by error, please contact the City and then shred the original document. Any use by others is strictly prohibited."

- h. Do not use or post customer's Social Security number as an account identifier or on any other documents unless requested by customer or required by federal law (such as W-2 forms).

2. **Steps to take when you Detect a Red Flag.** In the event City personnel detect Red Flags, they will take one or more of the below steps, commensurate with the degree of risk posed, to prevent and mitigate risk of Identity Theft. City personnel have the discretion to determine the degree of risk posed and to act accordingly.

- a. Continue to monitor an account for evidence of Identity Theft;
- b. Contact the customer either by written notice or telephone;
- c. Refuse to open a new account;
- d. Close an existing account;
- e. Reopen an account with a new number;
- f. Notify the Program Administrator for determination of the appropriate step(s) to take;
- g. Notify law enforcement; or

h. Determine that no response is warranted under the particular circumstances.

3. **Steps to take when you receive notice of an address**

discrepancy. In the event the City receives a notice of address discrepancy from a nationwide consumer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report, the City will reasonably confirm that an address is accurate by any of the following means:

- a. Verify the address with the consumer;
- b. Review City records;
- c. Verify the address through third-party sources; or
- d. Use other reasonable means to verify the address.

If an accurate address is confirmed, the City will furnish the consumer's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:

1. The City establishes a continuing relationship with the consumer; **and**
2. The City, regularly and in the ordinary course of business, furnishes information to the consumer reporting agency.

VIII. Service Provider Arrangements

In the event the City engages a service provider to perform an activity in connection with a Covered Account, the City will take one of the following steps to ensure the service provider performs in accordance with the Program:

1. Amending City contract templates to incorporate these requirements or
2. Determine through written acknowledgement that the service provider has reasonable alternative safeguards that provide the same or a greater level of protection for customer information as provided by the organization.

The above specified contracts shall include indemnification provisions limiting the City's liability for the service provider's failure to detect, prevent, or mitigate Identity Theft.

IX. Non-disclosure of Specific Practices

Disclosure of specific information or practices regarding Red Flag identification, detection, mitigation and prevention practices may be limited to designated City staff and/or policymakers. Documents produced to develop or implement the Program which describe specific practices may constitute Security Information and may be non-disclosable because disclosure would likely jeopardize the security of Identifying Information and may circumvent the City's Identity Theft prevention efforts.