Identity Theft Prevention Program

Effective November 1, 2008
Resolution #2008-_____

I. PROGRAM ADOPTION

The City of Calistoga 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.

The City of Calistoga provides water and wastewater utility services to all properties located within the City limits and properties outside of the City limits under specific conditions (referred to as "Utility").

This Program was developed by the Administrative Services Director ("Director") after consideration of the size and complexity of the Utility's operations and account systems, and the nature and scope of the Utility's activities. The Director has determined that this Program is appropriate for the City of Calistoga and the Program was initially reviewed and approved by the City Council of the City of Calistoga on October 21, 2008 by Resolution #2008-_____.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

Under the Red Flag Rule, every financial institution and creditor, such as the City of Calistoga, 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 Utility's accounts that are individual utility service accounts held by customers of the utility whether residential, commercial or industrial are covered by the Rule. Under the Rule, a "covered account" is:

1. Any account the Utility offers or maintains primarily for personal, family or household purposes, that involves 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.

"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 Utility 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 Utility identifies the following red flags, in each of the listed categories:

A. 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.
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.

B. 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 Utility that a customer is not receiving mail sent by the Utility;
6. Notice to the Utility that an account has unauthorized activity;
7. Breach in the Utility's computer system security; and
8. Unauthorized access to or use of customer account information.

C. Alerts from Others

Red Flag

1. 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.

IV. DETECTING RED FLAGS.

In order to detect any of the Red Flags identified above associated with the opening of a **new account**, Utility personnel will take the following steps to obtain and verify the identity of the person opening the account:

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);
3. Review documentation showing the existence of a business entity; and
4. Independently contact the customer.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Utility 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. Reopen an account with a new number;

7. Notify the Director 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.

Protect customer identifying information

In order to further prevent the likelihood of identity theft occurring with respect to Utility accounts, the Utility 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 that office computers are password protected
3. Keep offices clear of papers containing customer information;
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.

VI. PROGRAM UPDATES

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the security of the City utility system from Identity Theft. At least annually, the Director will review the past year experiences with any Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the City maintains and changes in the City's business arrangements with other entities. After considering these factors, the Director will determine whether changes to the Program are warranted. If warranted, the Director will update the Program and present the recommended changes to the City Council. The 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 Administrative Services Director. The Director will be responsible for the Program administration, for ensuring appropriate training of Utility 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

Utility staff responsible for implementing the Program shall be trained either by, or under the direction of, the Director in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

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 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 Utility's Program and report any Red Flags to the Director.

D. Specific Program Elements and Confidentiality

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 is to be limited to 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.