

**SILVER LAKE WATER & SEWER DISTRICT
IDENTITY THEFT PREVENTION PROGRAM**

I. PROGRAM ADOPTION

The Silver Lake Water & Sewer District ("District") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed with the oversight and approval of the District Board of Commissioners After consideration of the size and complexity of the District's operations and account systems, and the nature and scope of the District's activities, the District Board of Commissioners determined that this Program was appropriate for the District, and therefore approved this Program by the adoption of Resolution No. 634 on the 23rd day of October, 2008.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

Under the Red Flags Rule, the District is required to establish an identity theft prevention program tailored to its size, complexity and the nature of its operation. The Program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags as defined in the Rule and this Program for new and existing covered accounts and incorporate those Red Flags into the Program;
2. Provide for District staff efforts to 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. Update the Program periodically to reflect changes in risks of customers to identity theft or to the safety and soundness of the District's Program.

B. Red Flags Rule definitions used in this Program

For the purposes of this Program, the following definitions apply:

1. Account. "Account" means a continuing relationship established by a person with the District to obtain water and/or sewer or other service for personal, family, household or business purposes.
2. Covered Account. A "covered account" means:
 - a. Any account the District offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and

- b. Any other account the District offers or maintains for which there is a reasonably foreseeable risk to customers of identity theft or to the safety and soundness of the District's Program.
3. Creditor. "Creditor" has the same meaning as defined in Section 702 of the Equal Credit Opportunity Act, 15 U.S.C. 1691a, and includes a person or entity that arranges for the extension, renewal or continuation of credit, including the District.
4. Customer. A "customer" means a person or business entity that has a covered account with the District.
5. Financial Institution. "Financial institution" means a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a "transaction account" belonging to a customer.
6. Identifying Information. "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.
7. Identity Theft. "Identity Theft" means fraud committed using the identifying information of another person.
8. Program Administrator "Program Administrator means the District General Manager or his or her designee.
8. Red Flag. A "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft or attempts at Identity Theft.
9. Service Provider. "Service provider" means a person or business entity that provides a service directly to the District relating to or in connection with a covered account.

III. IDENTIFICATION OF RED FLAGS.

In order to identify relevant Red Flags, the District shall review and consider the types of covered accounts that it offers and maintains, the methods it provides to open covered accounts, the methods it provides to access its covered accounts, and Red Flags, in each of the listed categories as each pertains to District covered accounts:

A. 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.

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 a person's signature on a check appears forged); and

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides;
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a driver's license);
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. Failing to provide complete personal identifying information on an application when reminded to do so (**however, by law social security numbers may not be required**); and
6. Identifying information which 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 when such occurs without a demonstrated change in legal title to the premises provided water or sewer service by the District;
2. Payments stop on an otherwise consistently up-to-date account;
3. Mail sent to the account holder is repeatedly returned as undeliverable;
4. Notice to the District that a customer is not receiving mail sent by the District;
5. Notice to the District that an account has unauthorized activity;
6. Breach in the District's computer system security; and

7. Unauthorized access to or use of customer account information.

E. Alerts from Others

Red Flag

1. Notice to the District from a customer, a victim of identity theft, a law enforcement authority or other person that the District 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**, District personnel may take all or some of the following steps to obtain and verify the identity of the person opening the account:

Detect Red Flags

1. Require certain identifying information such as name, residential or business address, principal place of business for an entity, contact phone numbers or other identification;
2. Verify the customer's identity (for instance, confirm contact phone numbers;
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**, District personnel may take all or some of the following steps to monitor transactions with an account:

Detect Red Flags

Attempt to

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 District 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 Identity Theft

1. Monitor a covered account for evidence of Identity Theft;
2. Contact the customer with the covered account;
3. Change any passwords or other security codes and devices that permit access to a covered account;
4. Not open a new covered account;
5. Close an existing covered account;
6. Reopen a covered account with a new 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.

Protect Customer Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to District accounts, the District shall take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Secure the District website especially should internet bill paying be allowed;
2. Undertake complete and secure destruction of paper documents and computer files containing customer information;
3. Make office computers password protected and provide that computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer identifying information;
5. Do not request, use, maintain or keep all or any part of any customer social security numbers;
6. Maintain computer virus protection up to date; and
7. Require and keep only the kinds of customer information that are necessary for District purposes.
8. Redact sensitive identifying personal information such as but not limited to social security numbers, government issued driver's license or identification number or the like from any forms or documents received by the District.

VI. PROGRAM UPDATES

District staff shall periodically review and update the Program to reflect changes in risks of customers to Identity Theft and to the safety and soundness of the District's Program.. The Program Administrator shall periodically consider the District's experiences with Identity Theft,

changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the District maintains and changes in the District's business arrangements with other entities and service providers. After considering these factors, the Program Administrator shall determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator shall implement the updated Program and report such changes to the District Board of Commissioners.

VII. PROGRAM ADMINISTRATION.

A. Oversight

The Program Administrator shall be responsible for developing, implementing and updating the Program.

The Program Administrator shall be responsible for the Program administration, for appropriate training of District 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

District staff responsible for implementing the Program and any updates to it 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. Staff responsible to implement the Program shall provide reports to the Program Administrator on incidents of Identity Theft or attempts of Identity Theft.

C. Service Provider Arrangements

In the event the District engages a service provider to perform an activity in connection with one or more covered accounts, the District shall take the following steps to require that 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 acknowledge receipt and review of the Program and agree to perform its activities with respect to District covered accounts in compliance with the terms and conditions of the Program and with all instructions and directives issued by the Program Administrator relative to the Program; or
2. Require, by contract, that service providers acknowledge receipt and review of the Program and agree to perform its activities with respect to District covered accounts in compliance with the terms and conditions of the service provider's identity theft prevention program and will take appropriate action to prevent and mitigate identity theft; and that the service providers agree to report promptly to the District in writing if the service provider in connection with a District covered account detects an incident of

actual or attempted identity theft or is unable to resolve one or more Red Flags that the service provider detects in connection with a covered account.

D. Customer Identifying Information and Public Disclosure

The identifying information of District customers with covered accounts shall be kept confidential and shall be exempt from public disclosure to the maximum extent authorized by law, including RCW 42.56.230(4). The District Board of Commissioners also finds and determines that public disclosure of the District's specific practices to identify, detect, prevent and mitigate identify theft may compromise the effectiveness of such practices and hereby directs that, under the Program, knowledge of such specific practices shall be limited to the Program Administrator and those District employees and service providers who need to be aware of such practices for the purpose of preventing Identity Theft.