The Board of Directors of Scotts Valley Water District established an Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act ("FACT Act") of 2003; and,

The FACT Act requires that organizations that defer payments for goods or services implement a written program that provides for identification, detection, and response to patterns, practices, or specific activities ("Red Flags") that could be related to identity theft; and,

The Scotts Valley Water District ("SVWD") established 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 ("FACT Act") of 2003. The FACT Act requires that financial institutions and organizations that defer payments for goods or services implement written programs which provide for identification, detection, and response to patterns, practices, or specific activities ("Red Flags") that could be related to identity theft. These programs must be in place by May 1, 2009.

This Program was developed with oversight and approval of the SVWD Board of Directors. After consideration of the size and complexity of SVWD's operations and account systems, and the nature and scope of SVWD's activities, the Board of Directors determined that this Program was appropriate for the Scotts Valley Water District.

**Program Purpose and Definitions**
Under the Red Flag Rule, each program must contain reasonable policies and procedures to:

- Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
- Identify ways to detect Red Flags;
- Include appropriate responses to Red Flags detected;
- Implement training programs to ensure that staff understand the procedures necessary to identify, detect and mitigate identity theft;
- Ensure the Program is updated periodically to reflect changes in risks to customers or to the safety and soundness of SVWD from identity theft, and
- Include a process for administration and oversight of the 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 SVWD’s accounts that are individual utility service accounts held by customers of SVWD, whether residential, commercial or industrial, are covered by the Rule. Under the Rule, a "covered account" is:

- Any account SVWD offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions, and
- Any other account SVWD offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of SVWD 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.

**Identification & Detection**

In order to identify relevant Red Flags, SVWD 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 F.T.C. identifies 26 examples of Red Flags which fall into the five categories below. Listed under each category below are the Red Flags determined to be relevant to SVWD.

1. **Alerts, Notifications or Other Warnings Received from Credit Reporting Agencies or Service Providers**
   - Notice or report received from a credit reporting agency of fraud involving a customer or applicant;
1. Notice or report received from a credit reporting agency of a credit freeze on a customer or applicant;
   - Notice or report received from a credit reporting agency of an active military duty alert for a customer or applicant;
   - Notice or report received from a credit reporting agency of a Social Security Number (SSN) that has not been issued or belongs to a deceased person, and
   - Age or gender on a credit report that is clearly inconsistent with information provided to SVWD by the customer or applicant.

2. Presentation of Suspicious Documents
   - Identification document or card that appears to be forged, altered or inauthentic;
   - Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
   - The SSN provided is the same as that submitted by another customer;
   - 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
   - An application that appears to have been altered or forged.

3. Presentation of Suspicious Personal Identifying Information
   - Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
   - Identifying information presented that is inconsistent with other sources of information such as an address not matching an address on a credit report or an address or phone number that is the same as that of another person;
   - Identifying information presented that is consistent with fraudulent activity such as an invalid phone number, a phone number associated with a pager or answering service or a fictitious billing address;
   - Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
   - A person fails to provide complete personal identifying information when attempting to establish a new account or make a payment, and
   - A person refuses to provide proof of identity or provides identifying information not consistent with the information that is on file for the customer when inquiring about an existing account.

4. Suspicious Account Activity or Unusual Use of Account Red Flags
   - A person other than the account holder, or those authorized by the account holder to access account information, requests information or asks to make changes to an established account;
   - Change of address requested for an account followed by a request to change the account holder's name;
- A customer fails to make the first payment or makes an initial payment but no subsequent payments;
- Consumption occurs on an inactive or suspended account;
- Payments stop on an otherwise consistently up-to-date account;
- Mail sent by SVWD to the account holder is repeatedly returned as undeliverable;
- Notice to SVWD that a customer is not receiving mail sent by SVWD;
- Notice to SVWD that an account has unauthorized activity;
- Breach in SVWD’s computer system security, and
- Unauthorized access to or use of customer account information.

5. Alerts from Others

- Notice to SVWD from a customer of any of the following:
  - Their utility statements are not being received;
  - Unauthorized charges have been made to their utility account;
  - Unauthorized changes have been made to their utility account;
  - Fraudulent activity has occurred on a bank account that is used to make payments to SVWD, and
  - Notice to SVWD from a customer, identity theft victim, law enforcement or other person that SVWD has opened or is maintaining a fraudulent account for a person engaged in identity theft.

Response to Red Flags

Red Flags will be detected as SVWD Customer Service staff interact with customers and the contracted consumer reporting agency. During the following processes, staff may be alerted to and will respond to these Red Flags as directed below:

- When establishing a new account, a customer is asked to provide an SSN so Customer Service staff can run an identity verification report. Reports from the consumer reporting agency may contain Red Flags.
  - Response: Do not establish the customer utility account over the phone. Ask the customer to appear in person and provide a government-issued photo identification.
- When establishing a new account, a customer refuses to provide identification or provides suspicious documents for identification.
  - Response: These issues should be referred to the Accounting Manager immediately.
Answering customer inquiries on the phone, via email, or at the counter:

- Someone other than the account holder(s) may ask for information about an account or may ask to make changes to the information on the account. A customer may also refuse to verify their identity when asking about an account.

Response: Inform the customer that the account holder(s) must give permission for them to receive information about the utility account. Do not make changes to or provide any information about the account unless the account holder contacts the District, verifies their identity, and requests that the individual making the inquiry be added to the account as an authorized user. An exception may only be made if the service on the account has been interrupted for non-payment. In this instance, the Customer Service staff may provide the payment amount needed for reconnection of service.

Authorized access for District employees:

- Employees may submit requests for customer information to the Utility Billing system.

Response: All requests for direct access to the Continental Utility Billing system require approval by the Accounting Manager before the Information Technology (IT) provider is authorized to provide access. All access is username specific and password controlled, and access shall be limited to authorized District personnel. The Utility Billing module monitors account data and provides an audit trail of all changes made to a customer’s account. This information will be spot checked to ensure only authorized personnel are making changes to utility accounts.

Receiving notification that there is unauthorized activity associated with a customer account:

- Customers may call to alert the District about fraudulent activity related to their utility account and/or the bank account used to make payments on the account

Response: Verify the customer’s identity and notify the Accounting Manager immediately. Take the appropriate actions to correct the errors on the account, which may include:

- Issuing a service order to connect or disconnect services;
- Assisting the customer with cancellation of their payment method (Online Bill Pay);
- Updating personal information on the customer account;
- Updating the mailing address on the customer account;
- Updating account comments to document the fraudulent activity;
- Adding or changing a PIN on an account, and
- Notifying and working with law enforcement officials.

A meter read may reflect consumption on a suspended or inactive account.
**Response:** Issue a service order to confirm the read and disconnect service if unauthorized consumption has been identified. Ensure that all property management companies and other interested property owners have signed the SVWD Service Agreement to permit service to remain active between tenancies.

**Notification that a utility account has been established by a person engaged in identity theft:**

**Response:** These issues should be referred to the Accounting Manager immediately. The claim will be investigated and appropriate action, including notifying law enforcement officials, will be taken to resolve the issue.

**Prevention & Mitigation of Identity Theft**

To further prevent the likelihood of identity theft occurring with respect to customer utility account, SVWD will take the following steps with respect to its internal operating procedure to protect customer identifying information.

- Maintain appropriate custody of documents containing customer information;
- Ensure complete and secure destruction of paper documents and computer files containing customer information;
- Ensure that service providers who receive and process utility billing information have programs in place to detect and prevent identity theft;
- Ensure that its website is secure or provide clear notice that the website is not secure;
- Ensure computer virus protection is up to date, and
- Ensure that office computers are password protected and that computer screens lock after a set period of time.

**Program Administration and Oversight**

The Program will be reviewed at least annually and updated as needed based on the following events:

- Experience with identity theft;
- Changes to the types of accounts and/or payment programs offered, and
- Implementation of new systems and/or new vendor contracts.

The Accounting Manager will provide ongoing oversight of the Program and will at least annually report to the General Manager and the Board of Directors Business and Administrative Committee (“Committee”) on the effectiveness of the Program and recommendations for material changes to the Program. The General Manager and the Committee will review the annual report and approve recommended changes to the Program, both annually and on an as-needed basis.

The Office Supervisor will oversee the daily activities related to identity theft detection and prevention, and ensure that all Customer Service staff are trained to detect and respond to Red Flags.
Staff Training
Any employee with the ability to open a new account, or access an existing account, will receive training on identifying and detecting Red Flags and the appropriate response action. In the event that an instance of identity theft is suspected, Management personnel and other office employees will also receive training on the contents of this Program. As necessary employees will be retrained if the Program is updated to include new methods of identifying and detecting Red Flags, or if new response actions are implemented.

Service Provider Arrangements
In the event SVWD engages a service provider to perform an activity in connection with one or more accounts, SVWD will require that such service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft and that the service provider have such policies and procedures in place and attest in writing their compliance.

Specific Program Elements and Confidentiality
For the effectiveness of identity theft prevention programs, the Red Flag Rule envisions a degree of confidentiality regarding SVWD’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 the General Manager, Accounting Manager and 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.