SCOTTS VALLEY WATER DISTRICT
svwd.org svwater

Program

Type:	Finance / Customer Service		
Title:	**Identity Theft Prevention**		
Description:	Establishes procedures in compliance with the standards set by the Federal Trade Commission's Fair and Accurate Credit Transactions Act (FACTA) of 2003 Red Flags Rules		
Review Date:	11/10/21	**Initial Date:**	04/08/09
Review Cycle:	3 Years		

Under the FACTA Red Flags Rules the Scotts Valley Water District (District) is considered a creditor that maintains customer accounts and provides services that are billed retroactively. The District must maintain a written program, tailored to its size and nature of operations, to detect, prevent and mitigate Identity Theft.

Definitions

Identity Theft: Fraud committed using the identity of another person.

Covered Account: An individual account of any customer types (residential, commercial, etc.) established and held by District.

Account Holder: Person who has assumed financial responsibility for water service from an existing service connection.

Identity Information: Any name or number that is used to identify a person, including name, phone number, social security number, date of birth, driver's license or identification number, passport number, employer or taxpayer identification number, account number, credit or debit card number including unique electronic identification number such as a PIN, CVC or CVS code.

Account Information: Confidential data as established by the Water Code related to a Covered Account.

Program Elements

The District takes the following steps as part of its internal operating procedures and practices to prevent Identity Theft:

- Requiring only necessary Identity Information when opening a Covered Account.
- Providing Account Information only to the Account Holder or a person authorized by Account Holder.

- Limiting access to financial and utility billing software to certain job classifications. Appropriate access is assigned, password protected and managed by a designated job classification
- Entering all credit card transactions related to Covered Accounts directly into an integrated payment system provided by a contract service using the most current data security protocols including a time out for inactivity, encryption and tokenization.
- Requiring enrollment using account number, creation of a unique user ID, password and two factor authentication to access online Account Information.
- Using a vendor specialized in information technology and security to manage and monitor District's computer network and infrastructure. Following security protocols established by vendor.
- Prohibiting the sharing or posting of passwords to computer network or applications.
- Not displaying credit/debit card and bank account information on account statements and receipts.
- Not leaving documents that contain Identity Information or Account information unattended on workstations, shared work areas and printers.
- Ensuring proper destruction of all documents.
- Providing a secure storage location for all documents.

The program is reviewed and updated periodically as necessary to reflect changes in risks from Identity Theft.