

**RESOLUTION OF THE BOARD OF DIRECTORS OF THE  
VALLECITOS WATER DISTRICT APPROVING THE  
IDENTITY THEFT PREVENTION PROGRAM POLICY AND PROCEDURES  
(Red Flags Program)**

WHEREAS, the Board of Directors wish to establish policy and procedures for an Identity Theft Prevention Program; and

WHEREAS, the Fair and Accurate Credit Transaction Act of 2003 ("FACTA"), as implemented by the Red Flag rules, issued by the Federal Trade Commission (FTC), along with other federal agencies requires creditors of customer accounts to implement an Identity Theft Prevention Program by May 1, 2009; and

WHEREAS, as Vallecitos Water District (VWD), is a creditor because it provides services to customers prior to receipt of payment through customer accounts, including utility service accounts, which are maintained primarily for personal, family or household purposes and involve multiple payments or transactions, and for which there is a reasonably foreseeable risk of identity theft; and

WHEREAS, the Program is created to identify patterns, practices and specific activities that indicate the possible existence of identity theft which are considered, "Red Flags" and for responding to "Red Flags" when discovered; and


WHEREAS, any employee with the ability to open a new covered account, or access/manage/close an existing account will receive training on identifying and detection of "Red Flags"; and


WHEREAS, "Red Flags" refers to a pattern, practice or specific activity that indicates the possible existence of identity theft as defined in the Red Flag Rules of "FACTA"; and

WHEREAS, the General Manager, or his/her designee, is responsible for the oversight, development, implementation and administration of the Identity Theft Prevention Program.

PASSED AND ADOPTED by the Board of Directors of the Vallecitos Water District at a regular meeting held on this 15<sup>th</sup> day of April, 2009, by the following roll call vote:

- AYES: GENTRY, POLTL, SHELL, HANNAN
- NOES:
- ABSENT: FERGUSON
- ABSTAIN:

  
 \_\_\_\_\_  
 Trish Hannan, President  
 Board of Directors  
 Vallecitos Water District

ATTEST:  
  
 \_\_\_\_\_  
 William W. Rucker, Secretary  
 Board of Directors  
 Vallecitos Water District

**VALLECITOS WATER DISTRICT  
IDENTITY THEFT PREVENTION PROGRAM POLICY AND PROCEDURES  
(Red Flags Program)**

**STATEMENT OF NEED AND DEFINITION**

Identity Theft is the fraudulent use of an individual's personally identifying information. Identity theft presents a risk to our customers and therefore to our organization. The Federal Trade Commission, FTC, requires "Financial Institutions", and "creditors" with "covered accounts" to implement a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account, any existing covered account and all other accounts VWD determines that there is a reasonably foreseeable risk of identity theft. As an institution offering such, "covered accounts", this program reaffirms and formalizes the actions and processes Vallecitos Water District, VWD, takes to mitigate identity theft risks.

**PURPOSE**

The Fair and Accurate Credit Transaction Act of 2003 ("FACTA"), as implemented by the Red Flag Rules, issued by the Federal Trade Commission, FTC, along with other federal agencies requires creditors of customer accounts to implement an Identity Theft Prevention Program. Vallecitos Water District, VWD, is a creditor because it provides services to customers prior to receipt of payment through customer accounts, including utility service accounts, which are maintained primarily for personal, family or household purposes and involve multiple payments or transactions, and for which there is a reasonably foreseeable risk of identity theft.

The purpose of this Identify Theft Prevention Program is to detect, prevent and mitigate identity theft in connection with all customer accounts, taking into consideration the level of risk for identity theft given the services provided by VWD. This Program is created to identify patterns, practices and specific activities that indicate the possible existence of identity theft which are considered, "Red Flags". The Program outlines the procedures for detecting "Red Flags" and for responding to "Red Flags" when discovered.

**DEFINITION**

"Red Flag" refers to a pattern, practice or specific activity that indicates the possible existence of identity theft as defined in the Red Flag Rules of "FACTA".

"Identity Theft" refers to a fraud committed or attempted using the personal identifying information of another person without his/her authority.

"Customer account" refers to any account provided by VWD that is considered a "covered account" under the Red Flag Rules of "FACTA".

"Personal identifying information" refers to any information that may be used by VWD to identify a specific person, including, but not limited to, a social security number,

government issued driver's license or identification number, telephone number or address.

"Authenticate" refers to verifying the identity of an individual before sharing any information regarding that individual's account(s).

#### **IDENTIFICATION OF RED FLAGS**

Currently, there are approximately 26 events and/or occurrences that have been identified that can reasonably indicate the potential for Identity Theft. Many of these 26 events and/or occurrences specifically relate to using credit reports when opening an account or reporting customer payment history directly to credit reporting agencies; which VWD does not do at this time. After careful examination of our accounts, including the methods by which we open and access accounts, and our past experience with identity theft, the following events/occurrences reasonably indicated the potential for identity theft and should be considered, "Red Flags" for the purposes of this policy:

1. Documents provided for identification appear to have been altered or forged.
2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
3. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
4. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
5. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by VWD. For example:
  - a. The address on an application is the same as the address provided on a fraudulent application;
  - b. The phone number on an application is the same as the number provided on a fraudulent application.
6. The Social Security Number provided is the same as that submitted by other persons opening an account or other customers.
7. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
8. Personal identifying information provided is not consistent with personal identifying information that is on file with VWD.

9. If VWD uses challenge questions, the person opening the covered account or the existing customer cannot provide authenticating information beyond that which generally would be available from a wallet.
10. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
11. VWD is notified that the customer is not receiving paper account statements.
12. VWD is notified of unauthorized charges or transactions in connection with a customer's covered account.
13. VWD is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

#### **DETECTION OF RED FLAGS**

The following is a list of detection methods used by VWD to detect "Red Flags" during the opening of new accounts and the routine handling of existing accounts.

1. Obtain personal identifying information of an individual to verify his/her identity prior to opening an account. Types of information may include:  
Name, Address, Phone Number, Photo Identification/Driver's License or Social Security Number
2. Verify personal identification information when obtained using records on file with VWD
3. Authenticate the identity of customers when they are requesting information about their accounts prior to sharing any information.
4. Authenticate the identity of customers when they are requesting to make any changes to their accounts prior to making any changes.
5. Verify the validity of all billing address change requests
6. Verify all requests to change banking information used for payment purposes

#### **PREVENTION AND MITIGATION OF RED FLAGS (RESPONDING TO RED FLAGS)**

In the event a "Red Flag" is detected, VWD is committed to preventing the occurrence of identity theft and will take the appropriate steps to mitigate any impact caused thereby. In order to respond appropriately to the detection of a "Red Flag", VWD shall consider any and all circumstances that may heighten the risk of identity theft. After assessing the degree of risk posed, VWD will respond to the "Red Flag" in an

appropriate manner, using one or more of these procedures each time a "Red Flag" is detected:

- Monitoring the account for evidence of identity theft
- Contact the customer directly
- Change or add a password, security code or other device that provides access to the account
- Reopening an account with a new account number
- Close an existing account
- Not opening a new account
- Not attempting to collect on an account
- Not selling an account to a debt collector
- Notify law enforcement
- Determine that no response is warranted under the particular circumstances
- Ask the customer to appear in person with government issued identification
- Require a deposit to be paid before providing service in lieu of collecting sensitive data vulnerable to theft
- Update all account information
- Deactivate payment method
- Initiate an investigation

In addition to any of the above actions, the General Manager will be notified of any "Red Flags" discovered.

## **PROGRAM ADMINISTRATION**

### **I Training of Staff**

Any employee with the ability to open a new covered account, or access/manage/close an existing covered account will receive training on identifying and detection of "Red Flags". They will also be trained in the appropriate response actions in the event that an instance of identity theft is suspected. Key management personnel in appropriate departments will also receive training on the contents of this Program. As necessary, employees will receive annual training updates when the Program is updated to include new methods of identifying and detecting "Red Flags", or if VWD's technology or procedures change, or if new response actions are implemented. The training and participation of VWD staff is crucial to the effective implementation of this Program. The General Manager, or designee, will oversee all staff training to ensure adequate training and effective implementation of the Program.

### **II Program Review and Update**

VWD is committed to maintaining an Identity Theft Prevention Program that is current with the ever-changing crime of identify theft. VWD will reassess this Program on at least an annual basis. In reassessing this policy, VWD will add/delete "Red Flags" as

necessary to reflect changes in risks to customers or the safety and soundness of VWD from Identity Theft. The annual review of this program will consider;

- VWD's past experience with Identity theft
- Changes in methods of identity theft
- Changes in methods to detect, prevent, and mitigate identity theft;
- Changes in the types of accounts that VWD offers or maintains, and
- Changes in the business arrangements of VWD, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

The General Manager, or designee, may recommend modifications to the Program. However, any modification to the Program will not be implemented unless first approved by the Board of Directors.

### III Program Approval and Adoption

This Program has been reviewed and approved by VWD's Board of Directors. VWD's Board has assigned the General Manager to be responsible for the oversight, development, implementation and administration of the Program. Annually, the designated staff member will deliver an Annual Report that will address compliance of VWD with this Program. VWD's governing body is responsible for reviewing this report and approving material changes to the Program as necessary to address changing identity theft risks.

### IV Annual Reporting

The General Manager, or designee will provide an annual report to VWD's Board that details VWD's compliance with this Program. This report will address the following;

- Effectiveness of the policies and procedures of VWD in addressing the risk of identity theft in connection with opening new accounts and with respect to managing of existing accounts;
- Service provider arrangements
- Significant incidents involving identity theft and management's response, and
- Recommendations for material changes to the Program

### V Service Provider Oversight

Whenever VWD engages a service provider to perform any activity in connection with a covered account, the General Manager is responsible for ensuring that the activity is conducted in compliance with reasonable policies and procedures to detect, prevent and mitigate the risk of identity theft. VWD will require that contracts with applicable third-party service providers have policies and procedures to detect relevant "Red Flags" that may arise in the performance of the service provider's activities, and either report the "Red Flags" directly to VWD, or directly to take appropriate steps to prevent or mitigate the identity theft. In any case, all third-party providers will notify the General Manager of VWD immediately when they have identified a "Red Flag".

**ADDITIONAL SECURITY ACTIVITY AND INFORMATION**

VWD has a 50-year history of successfully operating a water utility. VWD has established and maintains significant practices that are supportive of their Identity Theft Prevention Program. These include;

1. Checking references and doing background checks before hiring employees who will have access to customer information
2. Limiting access to customer information to employees who have a business reason to see it.
3. Controlling access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis
4. Reducing the amount of confidential information seen on inquiry screens
5. Training employees to take basic steps to maintain the security, confidentiality and integrity of customer information, including;
  - a. Locking rooms and file cabinets where records are kept
  - b. Not sharing or openly posting employee passwords in work areas
  - c. Training customer service personnel on how to safeguard customer information
  - d. Reporting suspicious attempts to obtain customer information directly to a manager
6. Preventing terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures
7. Maintain a careful inventory of VWD's computers and their specific IP addresses, servers and any other equipment on which customer information may be stored
8. Procedures for securely backing up information including offsite storage in secure facility
9. Destruction of old computer hard drives, discs, CDs, magnetic tapes and servers
10. Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information which include;
  - a. Checking with software vendors regularly to get and install patches that resolve software vulnerabilities,
  - b. Using anti-virus and anti-spy ware software that updates automatically,
  - c. Maintaining up-to-date firewalls and reviewing reports on effectiveness of firewalls,
  - d. IT security includes screening emails via a separate company before delivery to VWD,
  - e. Only IT Department personnel are able to connect to the network from home, and this is accomplished with a VPN connection,
  - f. Promptly pass along information and instructions to employees regarding any new security risks or possible breaches.