

DIABLO WATER DISTRICT

REGULATION NO. 121

IDENTITY THEFT PREVENTION PROGRAM

Section I. Purpose.

- A. This regulation sets forth the policy for identity theft prevention pursuant to the Federal Trade Commission's Red Flags Rule which implements the Fair and Accurate Credit Transactions Act of 2003.
- B. Under the Red Flag Rules, creditors are required to establish an Identity Theft Prevention Program (the "Program") tailored to its size, complexity, and the nature of its operation. According to the rule, a municipal utility is a creditor subject to the requirements. 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.
 - 4. Ensure the Program is updated periodically to reflect changes in risks to customers and/or to the safety and soundness of the creditor for identity theft.

Section II. Policy.

A. Element I of the Policy - Identification of Red Flags –

1. In order to identify relevant Red Flags, the types of utility accounts, the methods used to open, change, and access accounts, as well as previous experience with identity theft has been taken into account. The following are the categories of Red Flags:

(a) Suspicious Documents

- (i) Identification document or card that appears to be forged, altered, or inauthentic.
- (ii) Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document.
- (iii) Identification is not consistent with the information that is on file for the customer.
- (iv) Other documentation with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged).
- (v) Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address).

- (b) Suspicious Activities
 - (i) Mail sent to the account holder is repeatedly returned as undeliverable.
 - (ii) Notice that an account has unauthorized activity.
 - (iii) Unauthorized access to or use of customer account information.
 - (iv) A customer refuses to provide proof of identity when asked.
- (c) Alerts from Others
 - (i) Notice of fraud from a customer, identity theft victim, law enforcement or other person.

2. Elements II and III – Detection of and Response to Red Flags –

- (a) Red Flags will be detected as Customer Service staff interacts with customers and third parties. An employee will be alerted to these Red Flags during the following processes:
 - (i) Establishing a new water service account - When establishing a new account, a customer is asked to provide their state issued driver's license number or identification card and date of birth for identification purposes.

Response: If the customer refuses to provide any of the required information on the application, the account will not be established.

- (ii) Reviewing customer identification in order to establish an account, process a payment, or enroll the customer for an automatic bank draft - Staff may be presented with documents that appear altered or inconsistent with the information provided by the customer.

Response: Do not establish the account or accept payment until the customer's identity has been confirmed.

- (iii) Answering customer inquiries on the phone, via email or fax, and at the counter - Someone other than the account holder or co-applicant may ask for information about a water service account or may ask to make changes to the information on an account. A customer may also refuse to verify their identity when asking about an account.

Response: Inform the customer that the account holder or the co-applicant must give permission for them to receive information about the water service account. Do not make changes to or provide any information about the account unless such permission has been granted by the account holder. Permission may be granted over the phone once validation of identification information has taken place. There can be only one PAYEE on an account. They may only receive information about the account, but are not allowed to make any changes to the account. The account holder or co-applicant are the only two that can ADD a PAYEE to the account.

- (iv) Receiving notification that there is unauthorized activity associated with a utility account, bank account, or credit card used to make payments on the account -
Customers or others may call to alert the District about fraudulent activity related to their water service account and/or the bank account or credit card used to make payments on the account.

Response: Verify the customer's identity and notify the Accounting Operations Manager immediately. Take the appropriate actions to correct the account which may include:

- a. Issuing a service order to connect or disconnect services. Assist the customer with deactivation of their payment method (automatic draft).
- b. Updating personal information on the water services account.
- c. Updating the mailing address on the water services account.
- d. Updating account notes to document the fraudulent activity.
- e. Adding a password to the account.
- f. Notifying and working with law enforcement officials.

(v) Receiving notification that a water service account has been established for a person engaged in identity theft

Response: Immediately notify the Accounting Operations Manager. The claim will be investigated,

and appropriate action will be taken to resolve the issue as quickly as possible.

3. Element IV – Updating the Program - This policy will be reviewed at least annually and updated as needed based on experience with identity theft, changes to the types of accounts and/or programs offered, and procedural changes.

Section III. Administration, Oversight and Training.

- A. The Accounting Operations Manager will oversee the daily activities related to identity theft detection and prevention and ensure that all members of Customer Service staff are trained to detect and respond to Red Flags. Training will occur annually, when the policy is revised or more frequently as situations of identity theft arise.
- B. The Accounting Operations Manager will review this policy with the General Manager annually. A report will be presented to the Board if any of the following material matters occur:
 1. Significant incidents involving identity theft and the response to those incidents.
 2. Recommendations of changes to the Program.

Section IV. Confidential Credit Card and Bank Account Information.

- A. Credit card and bank account information must be treated as confidential and must not be left unattended. All documents containing this information

must be locked when not in use. This confidential information may only be destroyed by shredding and in accordance with the Records Retention Policy.