

**OTAY WATER DISTRICT  
BOARD OF DIRECTORS POLICY**

Subject	Policy Number	Date Adopted	Date Revised
IDENTITY THEFT RED FLAGS POLICY	51	5/13/09	

**PURPOSE**

This policy is established to comply with regulations issued by the Federal Trade Commission (FTC), 16 CFR Part 681, as part of the implementation of the Fair and Accurate Credit Transaction Act of 2003 (FACTA). The FACTA requires that “financial institutions” and “creditors” with “covered accounts” implement written programs which provide for detection of and response to specific activities (“red flags”) that could be related to identity theft. An FTC rule notice states that creditors include “utility companies,” and provides that “utility accounts” are covered accounts.

**SCOPE**

The FTC regulations require the establishment of an Identity Theft Prevention Program (“Program”) that includes reasonable policies and procedures to:

1. Identify relevant red flags and incorporate them into the Program.
2. Detect red flags.
3. Include appropriate responses to red flags.
4. Address new and changing risks through periodic Program updates.
5. Include a process for administration and oversight of the Program.

**BACKGROUND**

Identity thieves use other person’s identifying information to open new accounts and misuse existing accounts, creating havoc for consumers and businesses. The FTC, the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations (the Red Flags Rules) requiring financial institutions and creditors to develop and implement written Identity Theft Prevention Programs as part of FACTA. The Programs must provide for the identification, detection, and response to patterns, practices, or specific activities – known as “red flags” – that could indicate identity theft.

**POLICY**

**1. Relevant Red Flags**

Red flags are warning signs or activities that alert a creditor to potential identity theft. The guidelines published by the FTC include 26 examples of red flags which fall into the five categories below:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers.

- Presentation of suspicious documents.
- Presentation of suspicious personal identifying information.
- Unusual use of, or other suspicious activity related to, a covered account.
- Notice from customers, victims of identity theft, or law enforcement authorities regarding possible identity theft in connection with customer accounts.

After reviewing the FTC guidelines and examples, staff determined that the following red flags are applicable to customer accounts. These red flags, and the appropriate responses, are the focus of this Program.

- Suspicious Documents and Activities:
  - Documents provided for identification appear to have been altered or forged.
  - The photograph, physical description, and/or other information on the identification is not consistent with the physical appearance of the person presenting the identification.
  - Information on the identification is not consistent with readily accessible information that is on file with the District.
  - The customer does not provide required identification documents when attempting to establish a utility account.
  - A customer refuses to provide proof of identity or appropriate security code information when discussing an established utility account.
  - A person other than the account holder or co-applicant requests information or asks to make changes to an established utility account.
  - Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the account.
- A customer notifies the District of any of the following activities:
  - Utility statements are not being received.
  - Unauthorized changes to a utility account.
  - Unauthorized charges on a utility account.
  - Fraudulent activity on the customer's bank account or credit card that is used to pay utility charges.
- The District is notified by a customer, a victim of identity theft, or a member of law enforcement that a utilities account has been opened for a person engaged in identity theft.

## **2. Detecting Red Flags**

Red flags may be detected as employees interact with customers during the routine handling of new and/or existing accounts. The following is a list of detection methods that the District may use to prevent identity theft.

- Require customers to present government-issued identification information to open a new account. Types of necessary information include:
  - Name
  - Address
  - Phone number
  - Photo identification
- Independently contact the customer (in the case of phone or internet setup of new accounts).
- When fielding a request to access and/or modify an existing account, verify identity of the customer by requesting specific pieces of personal identifying information (identification similar to that used to open the account that matches information on the Customer Information System).
- For online or automated phone system access of customer accounts, require the establishment of security codes and/or questions during the initial set-up of the account.

### **3. Responses to Red Flags**

If personnel identify a red flag associated with a new or existing customer account, one or more of the following actions will be taken to rectify the situation.

- Do not establish the utility account or make changes to an existing account until the customer's identity has been confirmed.
- For an existing account, the District may discontinue the services associated with that account and/or:
- Attempt to contact the customer independently, using information already on the Customer Information System.
- Continue to monitor the account for evidence of identity theft and contact the customer to discuss possible actions.
  - Change the passwords, security codes, or other security devices that permit access to an existing account.
  - Reopen an existing account with a new account number.
  - Close an existing account.
- Notify local law enforcement and provide them with all the relevant details associated with the event.

### **4. Periodic Program Review and Updates**

The Finance Department staff is required to prepare an annual report which addresses the effectiveness of the Program, documents significant incidents involving identity theft and related responses, provides updates related to external service providers, and includes

recommendations for material changes to the Program. Recommendations for changes will be based on the following:

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

#### **5. Administration and Oversight of the Program:**

Specific roles are as follows:

- The Customer Service Manager will oversee the daily activities related to identity theft detection and prevention, ensure that all members of the customer service staff are trained to detect and respond to red flags, and provide ongoing oversight to ensure that the Program is effective.
- The Chief Financial Officer will prepare the annual report, which reviews all aspects of the Program as described above, and submit the report to the General Manager.
- The General Manager will review the annual report and approve any recommended changes to the Program, both annually and on an as-needed basis.