ATTACHMENT A

Administrative Policy Manual

Policy No: D-2

Date: 11-04-08

Approved: IWA

SUBJECT: Identity Theft Prevention Program-Utilities Accounts

PURPOSE: This program is in response to and in compliance with the Fair and Accurate Credit Transaction (FACT) Act of 2003 and the final rules and guidelines for the FACT Act issued by the Federal Trade Commission and federal bank regulatory agencies in November 2007

General Policy:

This document was created in order to comply with regulations issued by the Federal Trade Commission (FTC) as part of the implementation of the Fair and Accurate Credit Transaction (FACT) Act of 2003. The FACT Act requires that financial institutions and creditors implement written programs which provide for detection of and response to specific activities ("red flags") that could be related to identity theft. These programs must be in place by November 1, 2008.

The FTC regulations require that the program must:

1. Identify relevant red flags and incorporate them into the program
2. Identify ways to 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

Provisions/Program Details:

A. 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:

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

2. Presentation of suspicious documents
3. Presentation of suspicious personal identifying information
4. Unusual use of, or other suspicious activity related to, a covered account
5. Notice from customers, victims of identity theft, or law enforcement authorities

B. After reviewing the FTC guidelines and examples, the Utility Billing Services Division determined that the following red flags are applicable to utility accounts. These red flags, and the appropriate responses, are the focus of this program.

1. A consumer credit reporting agency reports the following in response to a credit check request:
    a. Fraud or active duty alert
    b. Credit freeze
    c. The Social Security Number (SSN) is invalid or belongs to a deceased person
    d. The age or gender on the credit report is clearly inconsistent with information provided by the customer
2. Suspicious Documents and Activities
    a. Documents provided for identification appear to have been altered or forged.
    b. The photograph on the identification is not consistent with the physical appearance of the customer.
    c. Other information on the identification is not consistent with information provided by the customer.
    d. The SSN provided by the customer belongs to another customer in the Customer Information System (CIS).
    e. The customer does not provide required identification documents when attempting to establish a utility account or make a payment.
    f. A customer refuses to provide proof of identity when discussing an established utility account.
    g. A person other than the account holder or co-applicant requests information or asks to make changes to an established utility account.
    h. An employee requests access to the CIS system or information about a utility account, and the request is inconsistent with the rules in Administrative Regulation: Privacy of Utility Account Information.
3. A customer notifies the Utility Billing Services Division of any of the following activities:
    a. Utility statements are not being received
    b. Unauthorized changes to a utility account
    c. Unauthorized charges on a utility account

d. Fraudulent activity on the customer's bank account or credit card that is used to pay utility charges

4. The Utility Billing Services Division 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.

C. Detecting and Responding to Red Flags

Red flags will be reported by Utility Billing Services Division employees who interact with customers and the City's credit reporting agency through third-party collection agency. Employees will look for red flags during the following processes:

1. Reviewing customer identification in order to establish an account, process a payment, or enroll the customer in the automatic bank draft (ABD) program: The Customer Service Representatives (CSRs) may be presented with documents that appear altered or inconsistent with the information provided by the customer.

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

2. Answering customer inquiries on the phone, via email, and at the counter: Someone other than the account holder or co-applicant may ask for information about a utility account (including Online BillPay accounts) or may ask to make changes to the information on an account. A customer may also refuse to verify his/her identity when asking about an account.

   Response: Inform the customer that the account holder or the co-applicant must give permission to receive information about the utility account. Do not make changes to or provide any information about the account, with one exception: if the service on the account has been interrupted for non-payment, the CSR may provide the payment amount needed for reconnection of service.

3. Processing requests from City of Indio/Indio Water Authority employees: Employees may submit requests for information in the CIS system that is inconsistent with the rules outlined in Administrative Regulation: Privacy of Utility Account Information.

   Response: All requests for direct access to the CIS system are approved by the Fiscal Officer, so the Information Technology Division shall reject requests that have not received appropriate approval. All other requests for information from the CIS system should be reviewed to ensure that they do

not violate any part of the Privacy Policy. Requests that are inconsistent with the policy will be denied.

4. Receiving notification that there is unauthorized activity associated with a utility account: Customers may call to alert the City/IWA about fraudulent activity related to their utility 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 Fiscal Officer immediately. Take the appropriate actions to correct the errors on the account, which may include:
   a. Issuing a service order to connect or disconnect services
   b. Assisting the customer with deactivation of their payment method (ABD and Online BillPay)
   c. Updating personal information on the utility account
   d. Updating the mailing address on the utility account
   e. Updating account notes to document the fraudulent activity
   f. Adding a password to the account
   g. Notifying and working with law enforcement officials

5. Receiving notification that a utilities account has been established for a person engaged in identity theft.

   Response: These issues should be reported to the Fiscal Officer immediately. The claim will be investigated, and appropriate action will be taken to resolve the issue as quickly as possible.

D. Additional procedures that help to protect against identity theft include:

1. CIS system access is based on the role of the user. Only designated employees have access to the entire system.
2. Customers may access limited information about their utility account online and via the automated phone system. In order to access information online, customers must enroll using their utility account number and service address, and they must create a unique user identification and password.
3. The IWA/ Utility Billing Services Division will analyze alternatives to reduce paper receipts generated during credit card payment processing.
4. The IWA/ Utility Billing Services Division will ensure that contract service providers that receive and process utility billing information also have programs in place to detect and prevent identity theft.

E. Administration and Oversight of the Program

IWA/ Utility Billing Services Division 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. The program will be reviewed at least annually and updated as needed based on the following events:

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

F. Specific roles are as follows:

The Fiscal Officer will submit an annual report to the General Services Manager and the Public Works Director. The Fiscal Officer will also oversee the daily activities related to identity theft detection and prevention, and ensure that all staff in the Utility Division are trained to detect and respond to red flags.

The Public Works Director will review the annual report and approve any recommended changes to the program, both annually and on an as-needed basis.

The Indio Water Authority board shall approve the initial program.

Identity Theft Prevention Program for Water Utilities

Guidelines for Compliance with the FACTAct Red Flag Rules

Overview

The Fair and Accurate Credit Transactions Act, or "FACTAct" of 2003, took effect Jan. 1, 2008. Entities covered by the rule have until May 1, 2009, to implement programs to comply with the rule. The rule requires creditors, including utilities, establish identity theft prevention programs for covered accounts. Indio Water Authority adopted their policy November 4, 2008.

The final rule requires each financial institution and creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, to develop and implement an Identity Theft Prevention Program to combat identity theft.

All electric, water and gas utilities must establish a program that includes reasonable policies and procedures for detecting, preventing and mitigating identity theft. This program should enable the utility to:

- Identify relevant patterns, practices, and specific forms of activity that are red flags signaling possible identity theft and incorporate those red flags into the program
- Detect red flags that have been incorporated into the Program
- Take steps to prevent and mitigate identity theft
- Ensure the program is updated periodically to reflect changes in risks of identity theft

What Key Changes has IWA made?

- Removed all unauthorized H.T.E users from utilities application including Indio Police Department and Code Enforcement
- Updated software to handle two signers for each account and an Authorized agent
- Created a "Closed Account Form" to include verifications of last 4 digits of a customer's social security account number
- Customer Service Representatives can only see last 4 digits of social security numbers on screen
- Water applications only show last 4 digits of social security numbers
- Customer service representatives must verify over the phone and in person if they are speaking to the account holder by requiring the last four digits of the account holder's social security number

What does this mean to you?

- Know that our Indio Residents have secure identity with City of Indio/Indio Water authority on web site-online pay, over the phone, pay by phone system, and in person
- No employee can access utility information unless they have a purpose, open case, or subpoena

ATTACHMENT B

Administrative Policy Manual

Policy No: D-2

Date: 11-04-08

Approved: IWA

SUBJECT: Privacy Of Utility Account Information

PURPOSE: City of Indio/Indio Water Authority utility customers are required to provide personal information in order to receive utility services. The information supplied is not generally available to local government agencies but may be made available by Indio Law Enforcement Officials. Government Code Section 6254.16 specifically limits who has access to personal information gathered for utility billing purposes and under what circumstances that information may be released. The City of Indio/Indio Water Authority is establishing this privacy policy in accordance with the FACT Act.

General Policy:

Utility Customer information is strictly confidential and may not be disclosed or accessed for purposes other than provision of, and billing for, utilities unless done so pursuant to one of the listed exceptions. "Utility Customer Information" is hereby defined as including, but not limited to, the name of the utility customer, credit history, utility usage data, home address, telephone number, social security number, and driver's license number.

Provisions:

A. Exceptions: The name of a utility customer, his/her home address, and utility usage data only may be disclosed as follows:

1. To an agent or authorized family member of the person to whom the information pertains, upon the written designation or authorization of such person, signed by the utility customer.

2. To an officer or employee of the City of Indio/Indio Water Authority when necessary for the performance of his or her official duties.

3. To a consultant, under contract with the City/Authority, when necessary for the performance of services under said contract; provided, that the Department Head administering said contract approves such disclosure.

4. Upon a valid court order or subpoena.

5. Upon the request of an employee of the Indio Police Department or its Code Enforcement Division relative to an ongoing criminal or code enforcement investigations.

6. Upon determination by the City of Indio/ Indio Water Authority that the public interest in disclosure of the information clearly outweighs the public interest in nondisclosure. Reliance on this exception requires the expressed approval of the City Attorney's office.

7. Requests for approval from the City Attorney's office shall be submitted in writing. The City Manager's office shall receive a copy of all requests and responses.

B. Utility Customer Information Not Covered by Exceptions: Only the name of the utility customer, the home address of a utility customer, and utility usage data may be disclosed pursuant to one of the exceptions. Disclosure of additional utility customer information (i.e., including, but not limited to, credit history, telephone number, social security number, and driver's license number) will only be made pursuant to a valid court order or subpoena.

C. Other Law Enforcement/Government Agencies: Disclosure of Utility Customer Information will be made to other law enforcement or government agencies only pursuant to a valid court order or subpoena.