PHELAN PIÑON HILLS COMMUNITY SERVICES DISTRICT
RESOLUTION NO. 08-16

RESOLUTION OF THE BOARD OF DIRECTORS OF THE PHELAN PIÑON HILLS COMMUNITY SERVICES DISTRICT ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, the Federal Trade Commission ("FTC") has adopted regulations that require "creditors" holding consumer or other "covered accounts" (which are defined to mean any account where customer payment information is collected in order to bill for services rendered) to develop an Identity Theft Prevention Program that complies with those regulations; and

WHEREAS, because the Phelan Piñon Hills Community Services District (the "District") provides water service to its customers, it is a "creditor" under the application FTC regulations and must, therefore, comply with those regulations by adopting and implementing an Identity Theft Prevention Program; and

WHEREAS, the District's Board of Directors desires to take action to comply with the applicable FTC regulations by adopting an Identity Theft Prevention Program.

NOW, THEREFORE, IT IS RESOLVED that the District's Board of Directors hereby adopts, and directs District staff to implement, the following Identity Theft Prevention Program.

1. **Program Goals.** The District's Identity Theft Prevention Program (the "Program") shall endeavor to achieve the following goals:

   a. To identify relevant patterns, practices, and specific activities (referred to in this Program as "Red Flags") that signal possible identity theft relating to information maintained in the Agency's customers' accounts, both those currently existing and those accounts to be established in the future;

   b. To detect Red Flags after the Program has been implemented;

   c. To respond promptly and appropriately to detected Red Flags to prevent or mitigate identity theft relating to District customer account information; and

   d. To ensure the Program is updated periodically to reflect any necessary changes.

2. The Program.

a. The District shall assess the security of its current customer account system, with an emphasis on assessing the methods by which it opens and maintains customer accounts and customers' personal information, and on assessing the manner in which it provides access to customer accounts. That assessment shall include an analysis of any prior incidents of identity theft which the Agency has experienced.

b. The District shall maintain identifying information (address, social security number, etc.) for each customer so it can authenticate customers, monitor transactions, and verify the validity of customer requests, such as a change of address or service-related requests, including requests to terminate service.

c. The District shall establish a reporting system which allows District staff to discover potential Red Flags as they arise and to thereafter report them to the proper authorities, including law enforcement. This reporting system should specifically focus on the following Red Flags: alerts, notifications, or other warnings received from consumer reporting agencies or service providers; presentation of suspicious documents by a purported customer; presentation of suspicious personal identifying information by a purported customer, such as a specific address change; the unusual use of, or other suspicious activity related to, customer's account; and notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with the District's customer accounts.

d. The District shall adopt procedures which provide for appropriate responses to any detected Red Flags which are commensurate with the degree of risk posed. In determining an appropriate response, the District shall consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records or notice that a customer has provided information related to a customer's account to someone fraudulently claiming to represent the District. Appropriate responses include the following: i) monitoring customer accounts for evidence of identity theft, ii) contacting the customer, iii) changing from time to time any passwords, security codes, or other security devices that permit access to customer accounts, iv) reopening a customer account with a new account number, v) not opening a new customer account, vi) closing an existing customer account, vii) determining that no response is warranted under the particular circumstances. Any Red Flags should be brought to the General Manager's attention to determine the appropriate response(s) to be implemented promptly after detection.

e. The District's General Manager, or his or her designee, shall implement and administer the Program. The General Manager shall provide periodic reports to the Board of Directors on the effectiveness of the Program and shall ensure that all necessary District employees are properly trained to implement the Program.

f. The General Manager shall annually review the Program with appropriate District staff to determine if any revisions are needed. That review may include changes in identity theft methods and changes in methods to detect, prevent, and mitigate identity theft. The General Manager is hereby authorized and directed to make any necessary changes in the Program that are found to be necessary, provided that such changes must be reported to the Board of Directors at the first regular Board of Directors' meeting after the change is made.

APPROVED AND ADOPTED this 19th day of November, 2008.

AYES: Roberts, Johnson, Adams, Anderson, Morrissette
NOES: None
ABSTAIN: None
ABSENT: None

By: Mark Roberts
Mark Roberts, President

Attest: Debbie Bishop
Debbie Bishop, Board Secretary

PHELAN PINON HILLS
COMMUNITY SERVICES DISTRICT

Identity Theft Prevention Program

This program is in response to and in compliance with the Fair and Accurate Credit Transaction (FACT) Act of 2003

The final rules and guidelines for the FACT Act issued by the Federal Trade Commission and federal bank regulatory agencies in November 2007

Adopted November 19, 2008– Resolution 2008-16

Identity Theft Prevention Program

Purpose

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. (FTC granted a six-month delay until May 1, 2009).

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.

Program Details

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 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.

After reviewing the FTC guidelines and examples, the Billing Department 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 on the identification is not consistent with the physical appearance of the customer.
    - Other information on the identification is not consistent with information provided by the customer.
    - The customer does not provide required identification documents when attempting to establish an account or make a payment.
    - A customer refuses to provide proof of identity when discussing an established customer account.
    - A person other than the account holder or co-applicant requests information or asks to make changes to an established customer account.
- An employee receives a request for information about a customer account, and the request is inconsistent with the regular operating procedures.
- A customer notifies the Billing Department or General Manager of any of the following activities:
    - Unauthorized changes to a customer account.
    - Unauthorized charges on a customer account.
    - Customer statements are not being received.
    - Fraudulent activity on the customer's bank account or credit card that is used to pay customer charges.
- The Billing Department or General Manager is notified by a customer, a victim of identity theft, or a member of law enforcement that an account has been opened for a person engaged in identity theft.
- A collection agency reports the following in response to a collection request from the District:
    - Fraud or active duty alert.
    - Credit freeze.
    - The Social Security Number (SSN) is invalid or belongs to a deceased person.
    - The age or gender on the credit report is clearly inconsistent with information provided by the customer.

Detecting and Responding to Red Flags

Red flags will be detected as Phelan Piñon Hills Community Services District employees interact with customers and any real estate agents, property managers, banks, escrow companies, title co.'s and collection agencies. An employee will be alerted to these red flags during the following processes:

- Establishing a new customer account: When establishing a new account, a customer must appear in person, complete a new owner application, bring in escrow paperwork for staff verification, provide a SSN, Drivers License no. and proof of identity. Deposits are required from all new owners and tenants if they are unable to provide a letter from a qualifying water agency stating account was in good standing during the previous 12 months of service. Red flags may occur when the customer is unable to provide all of the necessary documentation listed above.

  Response: Do not establish customer account until customer is able to provide this information. Check PIMS (Property Information Management System) to verify owner information. A deposit may also be required In order to establish service.

- Reviewing customer identification in order to establish an account, process a payment, or enroll the customer in the Automatic Payment Plan (ACH debit): District may be presented with documents that appear altered or inconsistent with the information provided by the customer.

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

- 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 customer 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 customer account. Do not make changes to or provide information about the account.

- Processing Owner/Tenant Agreements: When an owner of a property rents or leases the property and requests the tenant pay for the water bill directly to the District both parties must complete their respective part of the two part agreement. These forms can be completed and signed in the District office where identification can be verified, or completed and signed in the

presence of a Notary Public. Tenant may be required to pay a deposit. Documents presented to the District may appear altered or inconsistent with the information on the account. Owner may designate a different tenant than the one completing the tenant portion. Person completing the owner portion not owner of record.

Response: Do not open new account in Tenant's name until all paperwork is received and identities have been verified. A deposit may be required in order to establish service.

- Processing new Agent/Bank owned requests: These requests have the same requirements as new owner accounts. The District requires the Agent to complete a new Agent application, provide a copy of the Agent/Bank or mortgage holder agreement to represent along with verifying identification.

  Response: Do not open new account in Agent's name until all paperwork is received and identification has been verified.

- Receiving notification that there is unauthorized activity associated with a customer account: Customers may call to alert the District about fraudulent activity related to their account and /or bank account used to make payments on the account.

  Response: Verify the customer's identity, and notify the Billing Department or General Manager immediately. Take the appropriate actions to correct the errors on the account, which may include:

    - Assisting the customer with deactivation of their payment method.
    - Updating personal information on the utility account.
    - Updating the mailing address on the utility account.
    - Updating account notes to document the fraudulent activity.
    - Adding a password to the account.
    - Notifying and working with law enforcement officials.

- Receiving notification that a customer's account has been established for a person engaged in identity theft:

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