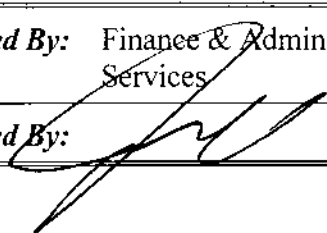




POLICY AND PROCEDURE

Subject: Identity Theft Prevention Program – Red Flags	Index: Finance Number: 201-6-2
Effective Date: December 15, 2009	Prepared By: Finance & Administrative Services
Supersedes: New	Approved By: 

1.0 PURPOSE:

To establish a policy for identity theft prevention pursuant to the Federal Trade Commission's Red Flag Rule which implements the Fair and Accurate Credit Transaction Act of 2003.

2.0 ORGANIZATIONS AFFECTED:

All departments and divisions.

3.0 REFERENCES:

Fair Credit and Reporting Act of 1971.
2003 Fair and Accurate Credit Transaction Act of 2003.
Records Management Program Policy 104-1.

4.0 POLICY:

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:

- Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program.
- Detect Red Flags identified in the Program and respond appropriately to prevent and mitigate identity theft.
- Maintain confidential information.
- 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.

5.0 **DEFINITIONS:**

- 5.1 Identity theft: The unauthorized use of personal consumer information, including name, address, bank account information, driver's license number, social security number, employment information, and other information used to identify an individual.
- 5.2 Red Flag Rule: The Federal Trade Commission has issued a set of regulations, known as the "Red Flags Rule," requiring that certain entities develop and implement written identity theft prevention and detection programs to protect consumers from identity theft.
- 5.3 Identity Theft Prevention Program: Required by the Federal Trade Commission, a formal written program of policies and actions to implement and maintain identity theft prevention by the City of San Clemente.
- 5.4 Red Flag: A Red Flag is a pattern, practice, or specific account activity that indicates the possibility of identity theft.
- 5.5 Notice of Fraud: A notification of fraudulent activity from a customer, identity theft victim, law enforcement, or credit reporting agency.
- 5.6 AutoPay: A payment option offered by Utility Billing which established a monthly Automated Clearing House draft from a consumer's bank account.

6.0 **PROCEDURE:**

6.1 Identification of Red Flags

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 have been taken into account. The following are the categories of Red Flags:

6.1.1 Suspicious Documents

- Identification document or card that appears to be forged, altered, or inauthentic.
- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document.
- Identification is not consistent with the information that is on file for the customer.
- Other documentation with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged)

- Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address).

6.1.2 Suspicious Activities

- Mail sent to the account holder is repeatedly returned as undeliverable.
- Notice that an account has unauthorized activity.
- Unauthorized access to or use of customer account information.
- A customer refuses to provide proof of identity when asked.

6.1.3 Alerts from Others

- Notice of fraud from a customer, identity theft victim, law enforcement or other person.

6.2 Detecting and Responding to Red Flags

Red Flags will be detected as Utility Billing staff interacts with customers and third parties. An employee will be alerted to these Red Flags during the following processes:

6.2.1 Establishing a new utility account

When establishing a new account over the phone, a customer is asked to provide their driver's license or identification number, date of birth, and last four digits of their social security number for identification purposes.

Response: If the customer refuses, they must present their identification in person. If the customer refuses to present their identification, the account will not be established.

6.2.2 Reviewing customer identification in order to establish an account, process a payment, or enroll 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.

6.2.3 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 utility 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 utility 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 been taken.

6.2.4 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 City 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 Utility Billing Coordinator, Finance Manager and Information Technology, or designee immediately. Take the appropriate actions to correct the account which may include:

- Issuing a service order to connect or disconnect services.
- Assist the customer with the deactivation of their payment method (AutoPay).
- 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.

6.2.5 Receiving notification that a utility account has been established for a person engaged in identity theft

Response: Immediately notify the Utility Billing Coordinator, Finance Manager and Information Technology, or designee. The claim will be investigated, and appropriate action will be taken to resolve the issue as quickly as possible.

6.3 Confidential Credit Card and Bank Account information

6.3.1 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 Management Program Policy.

6.3.2 Information Technology will maintain the appropriate data servers, firewalls, and related data processing systems to protect confidential information.

6.3.3 Information Technology shall maintain proper SSL Secure Transaction Certificates for WEB Point-of-Sale transactions.

6.4 Administration, Oversight and Training

The Utility Billing Coordinator will oversee the daily activities related to identity theft detection and prevention and ensure that all members of Utility Billing 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.

The Utility Billing Coordinator will prepare an annual report to the Assistant City Manager, Finance Manager, and Information Technology. This report will address material matters related to the program and evaluate such issues as:

- The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with utility billing accounts.
- Service provider arrangements.
- Significant incidents involving identity theft and the response to those incidents.
- Recommendations of material changes to the Program.

6.5 Policy Updates

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.