



# ADMINISTRATIVE REGULATION

## Office of the City Manager

Number	AR 312
Sections	1-7
Effective Date	5-1-2009
Responsible Department	Finance
Amended Date	February 2016
Review Date	February 2021

### **SUBJECT: *Identity Theft Prevention Procedures***

1. **Purpose:** To establish a procedure which provides for detection of and response to specific activities ("red flags") that could be related to identity theft.
2. **Authority:** To comply with regulations issued by the Federal Trade Commission (FTC) and federal bank regulatory agencies as part of the implementation of the "Fair and Accurate Credit Transactions Act" (FACTA) of 2003 and the "Red Flag Program Clarification Act of 2010" (S.3987), which requires that financial institutions and creditors implement a written program to prevent identify theft.
3. **Application:** The regulation shall apply to all departments and customer service representatives (CSR's) in those departments who handle billing or payment questions, or sign up customers for utilities and obtain certain information from customers as per Municipal Code Section 14.08.010 Application Form, or other miscellaneous receivable accounts including emergency medical services, especially those which the City has offered and accepted a payment plan, or has otherwise extended credit.
4. **Definitions:**
  - 4.1 **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 with examples below:
    - 4.1.1 Alerts, notifications or other warnings received from consumer reporting agencies or service providers such as:
      - A consumer credit reporting agency reports the following in response to a credit check request
      - 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
    - 4.1.2 Suspicious personal identification, such as suspicious address change. Examples include:
      - Address information on the identification is not consistent with information provided by the customer or available in the consumer credit report.
      - The SSN provided by the customer belongs to another customer in

the Utility or Accounts Receivable system, or has not been issued, or is listed on the Social Security Administration's Death master file.

- The SSN is the same as that submitted by other applicants or customers, or there is a lack of correlation between the SSN range and the date of birth.
- The customer does not provide required identification documents when attempting to establish a utility account or make a payment, and cannot provide authenticating information beyond that which generally would be available from a wallet or a consumer report.
- A customer refuses to provide proof of identity when discussing an established utility account, or in response to a notification that the application is not complete. Acceptable forms of identification are a valid California driver's license, a valid passport, or valid military identification. Note: A valid out of state driver's license may be considered when accompanied by other valid identifying documents.
- A person other than the account holder or co-applicant requests information, or asks to make changes to an established utility account.
- An employee who does not handle customer calls or payments, requests access to the Utility or Accounts Receivable system, or information about a utility account.
- Other information provided, such as fictitious mailing address, mail drop addresses, jail addresses, or invalid phone number, is associated with fraudulent activity.

4.1.3 Suspicious documents, examples include:

- Documents provided for identification that appear to be altered or forged.
- Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer.
- Identification on which the information is inconsistent with information provided by the applicant or customer.
- Identification on which the information is inconsistent with readily accessible information that is on file with the creditor, such as an AutoPay application signature or recent check.
- An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.

4.1.4 Unusual use of, or other suspicious activity related to, an account such as a customer notifying a CSR of any of the following activities:

- Unauthorized changes to a utility account.
- Unauthorized charges on a utility account.
- The customer fails to make the first payment, or makes an initial payment, but no subsequent payments.
- A change is made resulting in an account being used in a manner that is not consistent with established patterns, such as nonpayment when there is no history of late or missed payments.
- Mail sent to the customer is returned repeatedly as "undeliverable" although transactions continue to be conducted in connection with the customer's account.
- The city is notified that the customer is not receiving paper statements.
- The city is notified by a customer, law enforcement or other person,

that it has opened a fraudulent account for a person engaged in identity theft.

- 4.1.5 Notice from customers, victims of identity theft, or law enforcement authorities, regarding possible identity theft or phishing relating to a utilities or accounts receivable account.

5. **Policy:** It is the City's policy to:

- 5.1 Identify relevant red flags and incorporate them into the program.
- 5.2 Identify ways to detect red flags.
- 5.3 Include appropriate responses to red flags.
- 5.4 Address new and changing risks through periodic program updates.

6. **Responsibility:**

- 6.1 All CSR employees handling utility, and accounts receivable payments and records, will be responsible for detecting "Red Flags". Each CSR will determine, in his or her discretion, whether the red flags suggest a threat of identity theft and report such flags to their division manager. Each Department Head will be responsible for ensuring the compliance of their staff to this procedure.

7. **Procedures:** Red Flags may be identified by a CSR through the following processes:

- 7.1 **Establishing a new utility account** - When establishing a new account, a customer is asked to provide a SSN to the CSR for the extension of credit and provide information on payment history. If the City receives a credit report from the customer, and if this report from the credit reporting agency contains a red flag, the CSR should not immediately establish the utility account. The CSR should ask the customer to appear in person and provide government issued photo identification, as well as notify their supervisor.
- 7.2 **Reviewing customer identification in order to establish an account, process a payment, or enroll the customer in the AutoPay program** - If the CSR is presented with documents that appear altered or inconsistent with the information provided by the customer, the CSR should not establish the utility account, or change the payment method to "AutoPay" until the customer's identify has been confirmed. The CSR should also notify their supervisor.
- 7.3 **Answering customer inquiries on the phone, via email, and at the counter** - If someone other than the account holder or co-applicant asks for information about a utility account, or ask to make changes to the information on an account, or a customer refuses to verify their identity by providing certain information when asked about an account, the CSR should inform the customer that the account holder or the co-applicant must give permission for them to receive information about the utility account, or they need to provide additional evidence that they are an authorized account holder. The CSR should 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.
- 7.4 **Processing requests from non CSR City of Huntington Beach employees** - Various employees may submit requests for information in the Utility or Accounts Receivable system that are not public information. All requests for information contained in the billing system shall be reviewed by a manager prior to being released to any employee. Any access to the Accounts Receivable and Utility billing system for staff other than CSR's in the various departments who require it in their normal course of business, shall have to be approved by the Director of Finance or his/her designee.
- 7.5 **Receiving notification that there is unauthorized activity associated with a utility account** - If a customer calls 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, the CSR should verify the customer's identity, and notify their division manager immediately. The CSR would need to take the appropriate actions to correct the errors on the account, which may include:

- Requesting that service be connected or disconnected.
- Assisting the customer with deactivation of their payment method (AutoPay).
- Requesting that personal information on the utility account be updated.
- Requesting that the mailing address on the utility account be updated.
- Updating account notes to document the fraudulent activity and require additional security procedures to be taken.
- Notifying and working with HBPD and other law enforcement agencies as needed.

**7.6 Receiving notification that a utilities account has been established for a person engaged in identity theft** - If a CSR receives this notification, they should escalate it to their division manager immediately. The claim will be investigated, and appropriate action will be taken to resolve the issue as quickly as possible.

**7.7 Additional procedures that help to protect against identity theft include:**

7.7.1 System access is based on the role of the user. Only certain job classifications have access to the customer and payment information in the City's records.

7.7.2 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.

7.7.3 The Finance Department will investigate ways to reduce/eliminate receipts generated during payments to protect customer's identities.

7.7.4 The Finance Department will ensure that service providers that receive and process utility billing and payment information have programs in place to prevent identity theft.

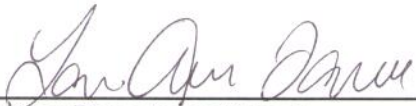
7.7.5 Ensure that office computers are password protected and that computer screens lock after a set period of time, or are locked when a staff leaves their PC.

7.7.6 Ensure complete and secure destruction of paper documents and computer files containing customer information.

7.7.7 Keep offices and cubicles clear of papers containing customer information and lock up key customer information.

7.7.8 Work with the Information Services Department to ensure that security software is kept up to date.

**7.8** Update this procedure periodically to reflect changes in risks from identity thefts based on an annual review of Red Flags identified during the prior fiscal year.



Initiating Department Head



Approved as to Form



Fred A. Wilson  
City Manager