Lake Havasu City

Identity Theft Prevention Program

Effective beginning May 1, 2009

I. PROGRAM ADOPTION

Lake Havasu City (City) developed this Identity Theft Prevention Program (Program) pursuant to the Federal Trade Commission's Red Flags Rule (Rule), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (16 C. F. R. § 681.2). This Program was developed with oversight and approval of the City Council. After consideration of the size and complexity of the City's operations and accounting systems, and the nature and scope of the City's activities, the City Council determined that this Program was appropriate for Lake Havasu City's Water and Wastewater Utilities in addition to other miscellaneous billings for covered accounts (including Airport, COBRA, After School Program, et al), and therefore approved this Program on April 28, 2009.

II. PURPOSE

The purpose of this Program is to protect the residents and customers of the City from identity theft. The Program is intended to establish reasonable policies and procedures to facilitate the detection, prevention, and mitigation of identity theft in connection with the opening of new Covered Accounts and activity on existing Covered Accounts.

III. SCOPE

This Program applies to the creation, modification, and access to Identifying Information of a customer of one or more of the services provided and operated by the City by any and all personnel of the City, including management personnel. This Program does not replace or repeal any previously existing policies or programs addressing some or all of the activities that are the subject of this Program, but rather is intended to supplement any such existing policies and programs.

IV. DEFINITIONS

When used in this Program, the following terms have the meanings set forth opposite their name, unless the context clearly requires that the term be given a different meaning:

Covered Account: The term "covered account" means: (1) any account a creditor (the City) offers or maintains primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or (2) any account a creditor (the City) offers or maintains for which there is a reasonably foreseeable risk to customers or the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks. For example, a City utility service account (water, sewer, et al) is a "covered account".

Identity Theft: The term "identity theft" means a fraud committed or attempted using the identifying information of another person without authority (16 CFR 603.2(a)).

Identifying Information: The term "identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including:

1. Name, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
2. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
3. Unique electronic identification number, address, or routing code; or
4. Telecommunication identifying information or access devise (as defined in 18 U.S.C. 1029(e)).

Using any single piece of information belonging to a real person falls within the definition of "identity theft".

Red Flag: The term "red flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Any other terms used but not otherwise defined herein shall have the meanings given to them in the FTC's Identity Theft Rules (16 CFR part 681) or the Fair Credit Reporting Act of 1970 (15 U.S.C. §1681 et seq.), as amended by the Fair and Accurate Credit Transactions Act of 2003 passed into law on December 4, 2003 (Public Law 108-159).

V. PROGRAM ADMINISTRATION

The initial adoption and approval of the Identity Theft Prevention Program shall be by resolution of the City Council. Thereafter, changes to the Program of a day-to-day operational character and decisions relating to the interpretation and implementation of the Program may be made by the Finance Director (Director) in consultation with the Compliance Auditor (Program Administrator). Major changes or shifts of policy positions under the Program shall only be made by the City Council.

Oversight

General/management oversight of the Program will be the responsibility of the Director. The Director may, but shall not be required to, appoint a committee to assist in administering the Program. The Director shall be the head of any such committee. Development, implementation, administration, and operational oversight of the Program will be the responsibility of the Program Administrator.

Staff Training and Reporting

Training on the Program will be provided by or under the direction of the Program Administrator each year for new employees who are expected to manage Covered Accounts.

The Program Administrator will report annually to the Director regarding compliance with this program. The report for each fiscal year will be submitted to the Director not later than September 30 of the subsequent fiscal year. The first report will address the condition of the Program during

the period from May 1, 2009, through June 30, 2010, and will be submitted not later than September 30, 2010. The Program Administrator may submit more frequent reports if circumstances warrant it.

Issues to be addressed in the annual Identity Theft Prevention Report include:

1. The effectiveness of the policies and procedures in addressing the risk of Identity Theft in connection with the opening of new Covered Accounts and activity with respect to existing Covered Accounts.
2. Service provider arrangements.
3. Significant incidents involving Identity Theft and management's response.
4. Recommendations for material changes to the Program, if needed for improvement.
5. Training sessions conducted and the departments and participants that attended training.

The Director will determine when major changes or shift of policy positions under the Program need to be presented to Council for approval.

VI. ELEMENTS OF IDENTITY THEFT PREVENTION

Identification of Relevant Red Flags

The City has considered the guidelines and the illustrative examples of possible Red Flags from the FTC's Identity Theft Rules and has reviewed the City's past history with instances of identity theft, if any. The City hereby determines that the following are the relevant Red Flags for purposes of this Program given the relative size of the City and the limited nature and scope of the services that the City provides to its residents/customers:

A. Alerts, notifications, or other warnings received from consumer reporting agencies, or service providers. (This subsection relates primarily to third-party service providers of the City, such as its collection agency.)

1. A fraud or active duty alert is included with a consumer report or an identity verification response from a credit reporting agency.
2. A consumer reporting agency provides a notice of address discrepancy, as defined in §681.1(b) of the FTC's Identity Theft Rules.

B. The presentation of suspicious documents.

3. Documents provided for identification appear to have been altered or forged.
4. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
5. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
6. Other information on the identification is not consistent with readily accessible information that is on file with the City.
7. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. The presentation of suspicious personal identifying information, such as a suspicious address change.

8. Personal identifying information provided is inconsistent when compared against external information sources used by the City. For example:
   a) The address does not match any address in existing publicly available records.
   b) The personal identifying information provided is associated with known fraudulent activity.
   c) The resident/customer fails to provide all needed personal identifying information upon request.
9. Personal identifying information provided by the resident/customer is not consistent with other personal identifying information provided by the resident/customer. For example, there is a lack of correlation between the dates of birth reflected on two different documents provided by the resident/customer.
10. Personal identifying information provided is associated with known or suspected fraudulent activity as indicated by internal or third-party sources used by the City.
11. The address, telephone number, or other expectedly unique identifying information provided is the same as that submitted by another person opening an account or another current resident/customer.
12. The person opening the account or the resident/customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
13. Personal identifying information provided is not consistent with personal identifying information that is on file with the City.
14. If the City uses identity verification questions, the person opening the account or the resident/customer cannot provide authenticating information beyond that which generally would be available from a wallet.

D. The unusual use of, or other suspicious activity related to, a Covered Account.

15. Shortly following the notice of a change of address for an account, the City receives a request for the addition of authorized users on the account.
16. A new account is used in a manner commonly associated with known patterns of fraud.
17. A covered account with a stable history shows irregularities.
18. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
19. Mail sent to the resident/customer is returned repeatedly as undeliverable although usage of products or services continues in connection with the resident/customer's covered account.
20. The City is notified that the resident/customer is not receiving account statements.
21. The City is notified of unauthorized usage of products or services in connection with a resident/customer's account.

E. Notice of Possible Identity Theft.

22. The City is notified by a resident/customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

Detection of Red Flags

The employees of the City that interact directly with residents/customers on a day-to-day basis shall have the initial responsibility for monitoring the information and documentation provided by the resident/customer and any third-party service provider in connection with the opening of new accounts and the modification of or access to existing accounts and the detection of any Red Flags that might arise.

Management shall see to it that all employees who might be called upon to assist a resident/customer with the opening of a new account or with modifying or otherwise accessing an existing account are properly trained such that they have a working familiarity with the relevant Red Flags identified in this Program so as to be able to recognize any Red Flags that might surface in connection with the transaction.

An employee who is not sufficiently trained to recognize the Red Flags identified in this Program shall not open a new account for any resident/customer, modify any existing account or otherwise provide any resident/customer with access to information in an existing account without the direct supervision and specific approval of a management employee.

Management employees shall be properly trained such that they can recognize the relevant Red Flags identified in this Program and exercise sound judgment in connection with the response to any unresolved Red Flags that may present themselves in connection with the opening of a new account or with modifying or accessing of an existing account. Management employees shall be responsible for making the final decision on any such unresolved Red Flags.

At the recommendation of the Program Administrator, the Director shall establish from time to time a written policy setting forth the manner in which a prospective new resident/customer may apply for service, the information and documentation to be provided by the prospective resident/customer in connection with an application for a new account, the steps to be taken by the employee assisting the customer with the application in verifying the resident/customer's identity, and the manner in which the information and documentation provided by the resident/customer and any third-party service provider shall be maintained. Such policy shall be generally consistent with the spirit of the Customer Identification Program rules (31 CFR 103.121) implementing Section 326(a) of the USA PATRIOT Act but need not be as detailed. At the recommendation of the Program Administrator, the Director shall establish from time to time a written policy setting forth the manner in which residents/customers with existing accounts shall establish their identity before being allowed to make modifications to or otherwise gain access to existing accounts.

Response to Detected Red Flags

If the responsible employees of the City as set forth in the previous section are unable, after making a good faith effort, to form a reasonable belief that they know the true identity of a resident/customer

attempting to open a new account or modify or otherwise access an existing account based on the information and documentation provided by the resident/customer and any third-party service provider, the City shall not open the new account or modify or otherwise provide access to the existing account as the case may be. City employees found to be discriminating against individuals with respect to opening of new accounts or the modification or access to existing accounts shall be subject to disciplinary action up to and including termination.

At the recommendation of the Program Administrator, the Director shall establish from time to time a written policy setting forth the steps to be taken in the event of an ongoing Red Flag situation. Consideration should be given to aggravating factors that may heighten the risk of Identity Theft, such as a data security incident that results in unauthorized access to an account, or a notice that a resident/customer has provided account information to a fraudulent individual or website. Appropriate responses to prevent or mitigate Identity Theft when a Red Flag is detected include:

1. Monitoring a Covered Account for evidence of Identity Theft.
2. Contacting the resident/customer.
3. Changing any passwords, security codes, or other security devices that permit access to a Covered Account.
4. Reopening a Covered Account with a new account number.
5. Not opening a new Covered Account.
6. Closing an existing Covered Account.
7. Not attempting to collect on a Covered Account or not selling a Covered Account to a debt collector.
8. Notifying law enforcement.
9. Determining that no response is warranted under the particular circumstances.

VII. PROGRAM MANAGEMENT AND ACCOUNTABILITY

Initial Risk Assessment – Covered Accounts

Utility accounts for personal, family and household purposes are specifically included within the definition of "covered account" in the FTC's Identity Theft Rules. Therefore, the City has determined that with respect to its residential and personal business accounts, it offers and/or maintains covered accounts. The City also performed an initial risk assessment to determine whether it offers or maintains any other accounts for which there are reasonably foreseeable risks to residents/customers or the City from identity theft. In making this determination, the City considered (1) the methods it uses to open its accounts, (2) the methods it uses to access its accounts, and (3) its previous experience with identity theft, and it concluded that its Accounting Division, Municipal Court and Parks & Recreation Department does offer or maintain other covered accounts.

Program Updates – Risk Assessment

The Program, including relevant Red Flags, is to be updated as often as necessary but at least annually to reflect changes in risks to customers from Identity Theft. Factors to consider in the Program update include:

1. An assessment of the risk factors identified above.
2. Any identified Red Flag weaknesses in associated account systems or procedures.
3. Changes in methods of Identity Theft.
4. Changes in methods to detect, prevent, and mitigate Identity Theft.
5. Changes in business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

Training and Oversight

All staff and third-party service providers performing any activity in connection with one or more Covered Accounts are to be provided appropriate training and receive effective oversight to ensure that the activity is conducted in accordance with policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

Other Legal Requirements

Awareness of the following related legal requirements should be maintained:

- 31 U.S.C. 5318 (g) – Reporting of Suspicious Activities
- 15 U.S.C. 1681 c-1 (h) – Identity Theft Prevention; Fraud Alerts and Active Duty Alerts – Limitations on Use of Information for Credit Extensions
- 15 U.S.C. 1681 s-2 – Responsibilities of Furnishers of Information to Consumer Reporting Agencies
- 15 U.S.C. 1681 m – Requirements on Use of Consumer Reports