City of Iowa Colony, Texas Identity Theft Prevention Program

Section 1. Policy and Purpose

The Federal Trade Commission adopted rules pertaining to an Identity Theft Prevention pursuant to the Red Flags Rule which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 which requires that creditors adopt an Identity Theft Prevention Program. The City Council of the City of Iowa Colony, Texas ("Council") has developed and hereby adopts this Identity Theft Prevention Program ("Program") as required by Part 681 of Title 16 of the Code of Federal Regulations ("Rule"), which implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed for the City of Iowa Colony, Texas ("City"). After consideration of the size and complexity of the City's operations and account systems and the nature and scope of the City's activities, the Council determined that the adoption of this Program is necessary to detect, prevent and mitigate identity theft in connection with the opening of or any existing Covered Accounts, as defined herein.

Section 2. Definitions

Unless otherwise noted, the following definitions follow the definitions included in the Rule.

A. Covered Account: Any account the Utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and any account the City offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the City from Identity Theft.
B. Creditors: Includes finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors.
C. City Personnel: The City's consultants and/or employees who use, maintain, collect or otherwise access Identifying Information in connection with a Covered Account.
D. Identity Theft: Fraud committed using the identifying information of another person without authority.
E. Identifying Information: Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing code.
F. Program: The Identity Theft Prevention Program for the City.
G. City Manager: The Council's operator is the City Manager.
H. Red Flag: A pattern, practice, or specific activity that indicates the possible existence of Identity Theft, as more fully described in this Program.

Section 3. Identification of Red Flags

To identify relevant Red Flags, the City has considered the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its

accounts, and its previous experiences with Identity Theft. The City has identified the following Red Flags:

A. Notifications and Warnings from Consumer Credit Reporting Agencies

1. Report of fraud accompanying a consumer credit report;
2. Active duty alert accompanying a consumer credit report;
3. Notice or report from a consumer credit agency of a credit freeze on a customer or applicant;
4. Notice or report of an address discrepancy from a consumer credit agency; and
5. Indication from a consumer credit report regarding activity that is inconsistent with a customer's usual pattern or activity, including but not limited to:
    a) Recent and significant increase in volume of inquiries;
    b) Unusual number of recent credit applications;
    c) A material change in use of credit; and
    d) Accounts closed for cause or abuse.

B. Suspicious Documents

1. Documents provided for identification that appear to be forged, altered or inauthentic;
2. Identification document or card containing a person's photograph or physical description that is not consistent with the appearance of the person presenting the document;
3. Other information on a document that is not consistent with information provided by a person opening a new account or existing customer information, such as if a person's signature on a check appears forged; and
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

1. An address or phone number presented that is the same as that of another customer or account;
2. An address presented that is fictitious, a mail drop or a prison;
3. A phone number that is invalid or associated with a pager or answering service;
4. Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates or phone numbers or lack of correlation between Social Security number range and date of birth);
5. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
6. Social Security number presented that is the same as one given by another customer;
7. A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law Social Security numbers may not be required) or an applicant cannot provide information requested beyond what could commonly be found in a purse or wallet; and
8. Identifying information that is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

1. Change of address for an account followed by a request to change the account holder's name;

2. Request for new/ additional services at multiple addresses;
3. Payments stop on an otherwise consistently up-to-date account;
4. Account used in a way that is not consistent with prior use (example: significant increase in water usage);
5. Mail sent to the account holder is repeatedly returned as undeliverable;
6. Notice to the City that a customer is not receiving mail sent by the City;
7. Notice to the City that an account has unauthorized activity;
8. Breach in the City's computer system security; and
9. Unauthorized access to or use of customer account information.

E. Alerts from Others

1. Notice to the City from a customer, Identity Theft victim, fraud detection service, law enforcement or other person that the City has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

Section 4. Detecting Red Flags

A. New Accounts. To detect any of the Red Flags identified above associated with the opening of a new account, City Personnel will take one or more of the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
2. Require that a customer service agreement be notarized;
3. Verify the customer's identity (for instance, review a driver's license or other identification card);
4. Review documentation showing the existence of a business entity;
5. Request additional documentation to establish identity; and
6. Independently contact the customer or business.

B. Existing Accounts. To detect any of the Red Flags identified above for an existing account, City Personnel will take one or more of the following steps to monitor transactions with an account:

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to close accounts or change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

Section 5. Preventing and Mitigating Identity Theft

In the event City Personnel detect any identified Red Flags, they may take one or more of the following steps, depending on the degree of risk posed by the Red Flag. In determining an appropriate response, the City Personnel will consider the number of Red Flags detected and any other factors that may heighten the risk of Identity Theft.

1. Continue to monitor an account for evidence of Identity Theft;
2. Contact all affected customers, through multiple methods if necessary;
3. Change any passwords or other security devices that permit access to an account;

4. Close an existing account;
5. Do not open a new account;
6. Do not close the account, but monitor or contact authorities;
7. Reopen an account with a new number;
8. Do not attempt to collect on the account;
9. Do not sell the account to a debt collector;
10. Notify the Program Administrator for determination of the appropriate step(s) to take;
11. Notify law enforcement; or
12. Determine that no response is warranted under the particular circumstances.

To further prevent the likelihood of identity theft occurring with respect to City accounts, the City Personnel will execute the following internal operating procedures to protect Identifying Information:

1. Ensure that any website through which or by which an exchange of information may be made is secure or provide clear notice that the website is not secure;
2. As allowed by law, ensure complete and secure destruction of paper documents and computer files containing customer information;
3. Ensure that office computers on which Covered Account information is stored or may be accessed are password protected and that computer screens lock after a set period of time;
4. Change passwords on office computers on which Covered Account information is stored or may be accessed on a regular basis;
5. Ensure all computers on which Covered Account information is stored or may be accessed are backed up properly and any backup information is secured;
6. Keep offices clear of papers containing customer information;
7. Request only the last 4 digits of social security numbers (if any);
8. Ensure computer virus protection is up to date for any computers on which Covered Account information is stored or may be accessed; and
9. Require and keep only the kinds of customer information that are necessary for City purposes.

Section 6. Program Administration and Oversight

The City Manager is responsible for developing, implementing, and updating this Program. The City Manager or his designee will be responsible for the Program administration, ensuring appropriate training of City Personnel, reviewing any reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances based on the degree of risk posed, and considering periodic updates to the Program.

Section 7. Staff Training

Initially, all City Personnel will be trained either by or under the direction of the City Manager or his designee in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. Thereafter, all City Personnel will undergo updated training not less than annually and all new City Personnel will undergo training.

Section 8. Reports and Program Updates

The Program will be periodically reviewed and updated to reflect changes in risks to customers and to the safety and soundness of the City from Identity Theft. The City Manager will submit a written report as necessary to the Council regarding the City's compliance with the Program and a recap of each incident of Identity Theft detection, including any prevention or mitigation steps taken. The City Manager will also evaluate the effectiveness of the Program in addressing Identity Theft risk; significant incidents of Identity Theft detection, including any prevention or mitigation steps taken; and recommendations for changes to the Program at least annually. In evaluating the program, the City Manager may consider, among other things, the City's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the City maintains, changes in the City's business arrangements with other entities, consultations with law enforcement authorities and/or agencies, and consultations with other City Personnel. After considering these factors, the City Manager will determine whether changes to the Program, including the list of Red Flags, are warranted. If warranted, the City Manager will present the Council with recommended changes and the Council will make a determination of whether to accept, modify or reject those changes to the Program.

Section 9. Service Provider Arrangements

In the event the City engages a service provider to perform an activity in connection with one or more Covered Accounts, the City will take steps to ensure that the service provider conducts its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft. Any such service provider will be provided with a copy of the Program and will be required to have such policies and procedures in place and to take appropriate steps to prevent or mitigate identity theft.

Section 10. Specific Program Elements and Confidentiality

For the effectiveness of Identity Theft Prevention Programs, the Rule envisions a degree of confidentiality regarding the City's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices is to be limited to the Council, the Program Administrator and City Personnel who need to know them for the purposes of preventing Identity Theft. Because this Program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program's general Red Flag detection, implementation and prevention practices are listed in this document.