CITY OF KENNEDALE

KENNEDALE
Finance Department

IDENTITY THEFT PREVENTION PROGRAM POLICY

ORIGINALLY ADOPTED BY CITY COUNCIL: NOVEMBER 13, 2008

PREFACE

The Federal Trade Commission (FTC) recently adopted rules on identity theft "red flags" (i.e., warning signs) pursuant to the Fair and Accurate Credit Transactions (FACT) Act of 2003. The new rules, which mandate action by November 1, 2008 (recently extended to May 1, 2009), require any business with a "covered account" to adopt and implement an identity theft program. Most cities that operate a municipal utility will be affected by these new rules.

A covered account is one where an entity (such as a municipal utility) provides a service or good before the consumer pays for it. For example, most municipal water utilities provide water to the customer, then the utility bills the customer later based on consumption.

A city with such accounts must adopt and implement a written program that: (1) identifies relevant identity theft "red flags" to the utility or other covered entity; (2) provides for detection of those red flags; (3) provides for appropriate responses to any red flags that are detected; and (4) ensures that the program is updated periodically to address changing risks.

Red flags may include unusual account activity, altered identity documents that are used to apply for an account, and a variety of other signs. Appropriate action in response to a red flag might include, among other actions, verification of personal information, contacting the customer, or other action that would prevent identity theft.

SUBSEQUENT REVIEW & ADOPTION

NOVEMBER 5, 2009
OCTOBER 14, 2010
OCTOBER 13, 2011
OCTOBER 3, 2012
OCTOBER 1, 2013
OCTOBER 13, 2014
OCTOBER 19, 2015
OCTOBER 17, 2016
JUNE 18, 2018

I. PROGRAM ADOPTION

The City of Kennedale ("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 for the Utility Department of the City ("Utility") with oversight and approval of the City Council. After consideration of the size and complexity of the Utility's operations and account systems, and the nature and scope of the Utility's activities, the City Council determined that this Program was appropriate for the City's Utility, and therefore approved this Program on November 13, 2008.

II. PURPOSE AND DEFINITIONS

A. Establish an Identity Theft Prevention Program

To establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003

B. Establishing and Fulfilling Requirements of the Red Flags Rule

The Red Flags Rule ("Rule") defines "Identity Theft" as "fraud committed using the identifying information of another person" and a "Red Flag" ("Red Flag") as a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

Under the Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. The Program must contain reasonable policies and procedures to:

1) Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
2) Detect Red Flags that have been incorporated into the Program;
3) Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4) Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from Identity Theft.

C. Red Flags Rule Definitions Used In This Program

1) City: The City of Kennedale, Texas.
2) Covered Account: Under the Rule, a "covered account" is:

a) Any account the Utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; or

b) Any other account the Utility offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Utility from Identity Theft.

3) Creditors: The Rule defines creditors "to include 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."

4) Identifying Information is defined under the Rule as "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.

5) Program: The Identity Theft Prevention Program for the City.

6) Program Administrator: The Director of Finance is the Program Administrator for the Program.

7) Utility: The Utility is the Utility Department for the City.

III. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the Utility considers 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 Utility identifies the following red flags, in each of the listed categories:

A. Notifications and Warnings From Consumer Credit Reporting Agencies

1) Red Flags

a) Report of fraud accompanying a consumer credit report;

b) Notice or report from a consumer credit agency of a credit freeze on a customer or applicant;

c) Notice or report from a consumer credit agency of an active duty alert for an applicant; and

d) Indication from a consumer credit report of activity that is inconsistent with a customer's usual pattern or activity, including but not limited to:

- Recent and significant increase in volume of inquiries
- Unusual number of recent credit applications
- A material change in use of credit
- Accounts closed for cause or abuse

B. Suspicious Documents

1) Red Flags

a) Identification document or card that appears to be forged, altered or inauthentic;
b) Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
c) Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and
d) Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

1) Red Flags

a) Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates, lack of correlation between Social Security number range and date of birth);
b) Identifying information presented that is inconsistent with other sources of information (for instance, Social Security number or an address not matching an address on a credit report);
c) Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
d) Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
e) Social Security number presented that is the same as one given by another customer;
f) An address or phone number presented that is the same as that of another person;
g) A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required) or an applicant cannot provide information requested beyond what could commonly be found in a purse or wallet; and
h) A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

1) Red Flags

a) Change of address for an account followed by a request to change the account holder's name;
b) Payments stop on an otherwise consistently up-to-date account;
c) Account used in a way that is not consistent with prior use (example: very high activity);
d) Mail sent to the account holder is repeatedly returned as undeliverable;
e) Notice to the Utility that a customer is not receiving mail sent by the Utility;
f) Notice to the Utility that an account has unauthorized activity;
g) Breach in the Utility's computer system security; and
h) Unauthorized access to or use of customer account information.

E. Alerts from Others

1) Red Flag

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

IV. DETECTING RED FLAGS

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new account, Utility personnel will take the following steps to obtain and verify the identity of the person opening the account:

1) Detect

a) 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;
b) Verify the customer's identity (for instance, review a driver's license or other identification card);
c) Review documentation showing the existence of a business entity;
d) Request additional documentation to establish identity; and
e) Independently contact the customer or business.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing account, Utility personnel will take the following steps to monitor transactions with an account:

2) Detect

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

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Utility personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

A. Prevent and Mitigate

1) Continue to monitor an account for evidence of Identity Theft;
2) Contact the customer, sometimes through multiple methods;
3) Change any passwords or other security devices that permit access to accounts;
4) Not open a new account;
5) Close an existing account;
6) Do not close the account, but monitor or contact authorities;
7) Reopen an account with a new number;
8) Notify the Program Administrator for determination of the appropriate step(s) to take;
9) Notify law enforcement; or
10) Determine that no response is warranted under the particular circumstances.

B. Protect Customer Identifying Information

In order to further prevent the likelihood of identity theft occurring with respect to Utility accounts, the Utility will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1) Ensure that its website is secure or provide clear notice that the website is not secure;
2) Where and when allowed, ensure complete and secure destruction of paper documents and computer files containing customer information;

3) Ensure that office computers are password protected and that computer screens lock after a set period of time;
4) Change passwords on office computers on a regular basis;
5) Ensure all computers 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; and
9) Require and keep only the kinds of customer information that are necessary for utility purposes.

VI. PROGRAM UPDATES

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the Utility from Identity Theft. Periodically, the Program Administrator will consider the Utility's experiences with Identity Theft situation, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the Utility maintains and changes in the Utility's business arrangements with other entities, consult with law enforcement authorities, and consult with other City personnel. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program or present the City Council with his or her recommended changes and the City Council will make a determination of whether to accept, modify or reject those changes to the Program.

VII. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee for the Utility. The Committee is headed by a Program Administrator who may be the head of the Utility or his or her appointee. Two or more other individuals appointed by the head of the Utility or the Program Administrator comprise the remainder of the committee membership. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of Utility staff on the Program, for reviewing any staff 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 and considering periodic changes to the Program.

B. Staff Training and Reports

Initially, all Utility staff shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. Thereafter, all Utility staff shall undergo update training not less than annually. Additionally, all new Utility employees shall undergo training.

All Utility staff shall submit reports as needed concerning the Utility's compliance with the program, the training that has been given and the effectiveness of the policies and procedures in addressing the risk of Identity Theft, including recommendations for changes to the Program. While incidents of Identity Theft are to be reported immediately to the Program Administrator, the reports shall contain a recap of the incident and include the steps taken to assist with resolution of the incident.

C. Service Provider Arrangements

In the event the Utility engages a service provider to perform an activity in connection with one or more accounts, including but not limited to franchise utility providers, the Utility will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1) Require, by contract or contract amendment, that service providers have such policies and procedures in place; and
2) Require, by contract or contract amendment, that service providers review the Utility's Program and report any Red Flags to the Program Administrator.

D. Specific Program Elements and Confidentiality

For the effectiveness of Identity Theft prevention Programs, the Red Flag Rule envisions a degree of confidentiality regarding the Utility'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 Identity Theft Committee and those employees who need to know them for 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.