CITY OF ANDREWS IDENTITY THEFT PREVENTION PROGRAM

Approved: February 26, 2010
Reviewed: March 18, 2015

I. PROGRAM ADOPTION

The City of Andrews ("Utility") developed this Identity Theft Prevention ("Program") pursuant to the Federal Trade Commission Red Flag Rules ("Rules"), which implement Section 114 of the Fair and Accurate Credit Transactions Act of 2003, 16 C. F. R. § 681.2. This Program was developed for the City of Andrews Finance Department.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

Under the Red Flags 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. Each 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.

B. Red Flags Rule Definitions Used in This Program

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

According to the rule, a utility is a creditor subject to the Rule requirements. 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."

All the Utility's accounts that are individual utility service accounts held by customers of the Utility whether residential, commercial or industrial are covered by the Rule. Under the Rule, a "covered account" is:

1. Any account the Utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. 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.

"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.

III. <u>IDENTIFICATION OF RED FLAGS</u>

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. Suspicious Documents

<u>Red Flags</u>

- 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;
- 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
- Application for service that appears to have been altered or forged.

B. Suspicious Personal Identifying Information

<u>Red Flags</u>

- Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
- Identifying information presented that is inconsistent with other sources of information (example: an address not matching an address on a credit report);
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;

- Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
- Social security number presented that is the same as one given by another customer;
- A person fails to provide complete personal identifying information on an application when reminded to do so; and
- A person's identifying information is not consistent with the information that is on file for the customer.

C. Suspicious Account Activity or Unusual Use of Account

Red Flags

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

D. Alerts from Others

Red Flag

- Notice to the Utility from a customer, identity theft victim, 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:

Detect

- 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

- Verify the customer's identity (for instance, review a driver's license or other identification card);
- Review documentation showing the existence of a business entity; and
- Independently contact the customer at residence (through backflow inspection).

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.

Detect

- Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
- Verify the validity of requests to change billing addresses; and
- 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:

Prevent and Mitigate

- Continue to monitor an account for evidence of identity theft;
- Contact the customer;
- Change any passwords or other security devices that permit access to accounts;
- Not open a new account
- Close an existing account;
- Reopen an account with a new number;
- Notify the Program Administrator for determination of the appropriate step(s) to take;
- Notify local law enforcement; and
- Determine that no response is warranted under the particular circumstances.

Protect Customer Identifying Information

- Ensure that the website is secure or provide clear notice that the website is not secure;
- Ensure complete and secure destruction of paper documents and computer files containing customer information;
- Require and keep only the kinds of customer information that are necessary for Utility purposes;

- Ensure that employees will not leave sensitive papers on their desks when not at work stations;
- Visitors entering areas where sensitive files are kept will be escorted by an employee;
- Require that entry codes or unescorted access will only be given to visitors when necessary;
- Take measures to protect and encrypt sensitive information stored on computers;
- Encrypt email transmissions with personally identifying information;
- Install anti-virus and anti-spyware programs on any computers that run on Utility servers or networks and ensure that programs are periodically updated;
- Ensure access to sensitive information will be controlled using passwords considered "strong" and passwords must be periodically changed;
- Require that passwords not be shared or posted;
- Any newly-installed software will have default passwords immediately changed;
- Require records containing sensitive information be shredded before placement in trash;
- When disposing of old computers and other electronic storage devices, use a disc wiping utility program.

Identifying information is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.

The following information is collected by this utility:

- Name
- Social Security Number
- Date of Birth
- Address
- Telephone number
- Driver's license identification number
- Alien registration number
- Government passport number
- Employer or taxpayer identification number

Customer personally identifying information is collected by the following methods:

- Presentation by customer at office
- Telephone
- Internet
- Mail

VI. <u>PROGRAM UPDATES</u>

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the Utility from identity theft. At least <u>annually,</u> 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. 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.

VII. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the Director of Finance/Program Administrator who is a senior management employee of the Utility. The Director of Finance/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

Utility staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator or his designee in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. Initial training will occur at the time of hiring by the Utility. Additional training will occur annually after the Identity Theft Prevention Program is updated each year.

The following specific measures will ensure the protection of individual information through staff training and procedures:

- Check references and/or do background checks of any new hires who will have access to sensitive information;
- Limit access to sensitive information to necessary employees only;
- Ensure that former employees no longer have access to sensitive information, such as collecting keys and terminating passwords;
- Employees required to notify management immediately if there is a potential security breach;
- Implement disciplinary action, including dismissal, for those employees who violate security policies.

C. Service Provider Arrangements

In the event the Utility engages a service provider to perform an activity in connection with one or more accounts, 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:

- Require that service providers have such policies and procedures in place; and
- Require that service providers review the Utility's Program and report any Red Flags to the Program Administrator;
- Require that service providers notify the Program Administrator of any security incidents, even if such incidents had not led to any confirmed compromise of the Utility's data.

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 those employees who need to know them for purposes of preventing Identity Theft. Because this program is 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.