

RESOLUTION No. 11-06-2010

A RESOLUTION OF THE CITY COUNCIL OF SANTAQUIN, UTAH ESTABLISHING AN IDENTITY THEFT POLICY IN COMPLIANCE WITH RECENT FEDERAL AND STATE LEGISLATION AND REGULATION.

WHEREAS, the Federal Trade Commission issued regulations on November 9, 2007 requiring creditors that hold consumer accounts to develop and implement a written identity theft prevention program providing for the identification, detection and response to patterns, practices or specific activities know as "Red Flags" that could indicate identity theft; and

WHEREAS, the compliance with these "Red Flag" rules is required by December 31, 2010; and

WHEREAS, The General Assembly of the State of Utah approved the "Protection of Personal Information Act" (the "Act"), effective January 1, 2007; and

WHEREAS, the implementation of both the "Red Flag Rules" and the "Act" require the City to establish policies limiting and managing the collection and dissemination of personal identifying and financial information, and the diligent pursuit of "red flags" which are indicators that identity theft is about to happen or has happened in the past in relation to our covered accounts;

NOW THEREFORE, BE IT RESOLVED by the City Council of Santaquin, Utah that:

1. The attached "Identity Theft Prevention Policy" (the "Policy") is hereby adopted with an effective date of November 18, 2010.
2. The Mayor is hereby authorized to make changes to this policy as necessary to achieve and maintain compliance with the letter and spirit of these requirements.

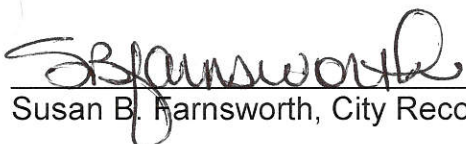
DATED this 17th day of November, 2010



SANTAQUIN CITY


James E. DeGraffenried, Mayor

Attest


Susan B. Farnsworth, City Recorder



Santaquin City Corporation
Identity Theft Prevention Program

Effective 17 November 2010

I. PROGRAM ADOPTION

Santaquin City Corporation ("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 operation and accounting for its utility services and the nature and scope of the utility services' activities, the City Council determined that this Program was appropriate for Santaquin City Corporation and therefore approved this Program on November 17, 2010

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

Under the Red Flag 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, municipal utilities are 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 City'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 City offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. Any other 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.

“Identifying information” is defined under the Rule and “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 number, employer or taxpayer identification number, unique electronic identification number, computer’s Internet Protocol address, or routing code.

III. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the City 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 experience with Identity Theft. The City identifies the following red flags, in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies

Red Flags

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on a customer or applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant; and/or
4. Indication from a credit report of activity that is inconsistent with a customer’s usual pattern or activity.

B. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a persons’ photograph or physical description is not consistent with the person presenting the document;
3. 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/or
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another customer;
6. An address or phone number presented that is the same as that of another person;
7. 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);
8. 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

Red Flags

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

E. Alerts from Others

Red Flag

Notice to the City 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**, City personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect

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. Verify the customer's identity (for instance, review a driver's license or other identification card);
3. Review documentation showing the existence of a business entity;
4. Independently contact the customer; and/or
5. Documentation showing ownership such as closing papers or warranty deed or lease agreement.

B. Existing Accounts

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

Detect

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 change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event City 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 Flags:

Prevent and Mitigate

1. Continue to monitor an account for evidence of Identity Theft;
2. Contact the customer;
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. Reopen an account with a new number;

7. Notify the Program Administrator for determination of the appropriate step(s) to take;
8. Notify law enforcement; or
9. Determine that no response is warranted under the particular circumstances.

Protect customer identifying information

In order to further prevent the likelihood of Identity Theft occurring with respect to City accounts, the City will take the following steps with respect to its internal operating procedures to protect customers identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. 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. Keep offices clear of papers containing customer information;
5. Truncation of social security number so only the last 4 digits are available;
6. Ensure computer virus protection is up to date; and/or
7. Require and keep only the kinds of customer information that are necessary for utility purposes.

VI. PROGRAM UPDATES

The City Treasurer will periodically review and update the Program to reflect changes in risks to customers and the soundness of the City from Identity Theft. In doing so, the City Treasurer will consider the City's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the City's business arrangements with other entities. After considering these factors the City Treasurer will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the City Treasurer will update the Program or present the City Council with his or her recommended changes and 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 City. The Committee is headed by the City Treasurer who may be the head of the City or his or her appointee. Two or more other individuals appointed by the head of the City or the City Treasurer will comprise the remainder of the committee membership. The City Treasurer will be

responsible for the Program administration, for ensuring appropriate training of City 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

City staff responsible for implementing the Program shall be trained either by or under the direction of the City Treasurer in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. *(The City may include in its Program how often training is to occur. The Program may also require staff to provide reports to the City Treasurer on incidents of Identity Theft, the City's compliance with the Program and the effectiveness of the Program.)*

C. Service Provider Arrangements

In the event the City engages a service provider to perform an activity in connection with one or more accounts, the City 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, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review the City's Program and report any Red Flags to the Program Administrator.

D. Non-disclosure of Specific Practices

For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices must be limited to the Identity Theft Committee who developed this Program and to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and in the information those documents contain are considered "security information" as defined under Utah Stat Code and are unavailable to the public because disclosure of them would be likely to substantially jeopardize the security of information against improper use, that use being to circumvent the City's Identity Theft prevention efforts in order to facilitate the commission of Identity Theft.