IDENTITY THEFT PREVENTION PROGRAM

For Rapid City

CITY OF RAPID CITY

Identity Theft Prevention Program

Effective beginning May 1, 2009

Jim Preston
Program Administrator

I. INTRODUCTION

The City of Rapid City developed this Identity Theft Prevention 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 Program Administrator. 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 Program Administrator determined that this Program was appropriate for the City of Rapid City, and therefore approved this Program on April 20, 2009.

II. PROGRAM APPLICATION

All individual municipal utility accounts, whether residential, commercial or industrial are covered by this Program. Therefore, reasonable policies and procedures for identification, detection and response to identity theft will be developed and maintained for training employees.

III. IDENTIFICATION OF RED FLAGS

The Red Flags Rule defines "Identity Theft" as "fraud using "identifying information" of another person. "Identifying information" specifically includes: 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, routing code.

The City of Rapid City identifies the following red flags, in each of the listed categories:

A. 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); and
8. A person's identifying information is not consistent with the information that is on file for the customer.

B. 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 holder is repeatedly returned as undeliverable;
5. Notice that a customer is not receiving mail sent by the Utility;
6. Notice that an account has unauthorized activity;
7. Breach in the computer system security;
8. Unauthorized access to or use of customer account information.

C. Alerts from Others

Red Flag

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

IV. DETECTION OF RED FLAGS

A. New Accounts

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

Detect

1. Require 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);

B. Existing Accounts

In order to detect any of the Red Flags identified above for an **existing account**, 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. RESPONDING TO RED FLAGS--PREVENTING AND MITIGATING THEFT

In the event 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;
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.

B. Protect customer-identifying information

In order to further prevent the likelihood of identity theft occurring with respect to Utility accounts, the City of Rapid City 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. Ensure complete and secure destruction of customer information;
3. Ensure that computers are password protected and computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer information;
5. Request only the last 4 digits of social security numbers (if any);
6. Ensure computer virus protection is up to date;
7. 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 City of Rapid City from Identity Theft. At least annually, the Program Administrator will consider the experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts maintained and changes in 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 or present the Rapid City Council with recommended changes and the Rapid 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 of Rapid City. The Identity Theft Committee will consist of the Finance Officer (or designee,) the Public Works Director (or designee,) and the City Attorney (or designee.) The Finance Officer (or designee) will serve as the Program Administrator heading the Committee. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of 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

Staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in Red Flag detection, and responsive steps to be taken when a Red Flag is detected.

C. Service Provider Arrangements

In the event the City engages a service provider to perform an activity in connection utility 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.