

Town of Readsboro

ORIGINAL
3/25/09 10:07 AM

Identity Theft Prevention Program
Water, Sewer and Electric Departments

Effective beginning May 1, 2009



ORIGINAL

I. PROGRAM ADOPTION

The entity designated on the cover page (hereinafter "Utility"), a Vermont municipal entity offering various utility services, has 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 in connection with those services. 16 C. F. R. § 681.2. This Program was developed with oversight and approval of the governing body of the Utility in accordance with law, with assistance from the Vermont Public Power Supply Authority. 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 Selectboard determined that this Program was appropriate for the Utility, and therefore approved this Program to take effect on May 1, 2009.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

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. 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 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."

Under the Rule, 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."

A "covered account" under the Rule consists of:

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. 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 credit reporting agencies (only to the extent Utility may utilize the services of such 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
- 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 person’s photograph or physical description is significantly inconsistent with the appearance of 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
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 materially inconsistent with other information the customer provides (i.e., inconsistent birth dates);
2. Identifying information presented that is materially 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. An address or phone number presented that is the same as that of another person, under circumstances that create a reasonable suspicion that the information given is untrue;
6. Failure of a person 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
7. Identifying information that is materially inconsistent 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 without explanation 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 to the Utility that a customer is not receiving mail sent by the Utility;
6. Notice to the Utility that an account has unauthorized activity;
7. Unauthorized access to or use of customer account information.

E. Alerts from others

Red Flag

1. Notice to the Utility from a customer, identity theft victim, law enforcement or other person that the Utility 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 as appropriate under the circumstances 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. Review documentation showing the existence of a business entity; and
3. In instances where the person requesting the account may not live within the service territory of the utility (for example, in the case of second home purchasers), take reasonable and appropriate steps to verify customer identity and information, taking into account the totality of the circumstances presented.

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

1. To the extent appropriate under the circumstances, verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);

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 Utility's good faith assessment of the degree of risk posed by the Red Flag, and other requirements imposed on the Utility by applicable law:

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 to the extent permitted by applicable law;

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 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 any website the Utility may maintain is secure, or provide clear notice that the website is not secure;
2. Ensure secure destruction of paper documents and computer files containing customer information at such time as destruction becomes appropriate;
3. Ensure that office computers are password protected and that computer screens lock after a set period of time;
4. Keep publicly accessible areas of offices clear of papers containing customer information;
5. Ensure computer virus protection is up to date; and
6. Require and keep only the kinds of customer information necessary for utility purposes.

VI. PROGRAM UPDATES

The Program Administrator will periodically review and update this Program to reflect changes in risks to customers and the soundness of the Utility from Identity Theft. In doing so, the Program Administrator will consider the Utility's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, 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. The Program Administrator will review the Program, and update it as warranted, at least once a year.

VII. PROGRAM ADMINISTRATION.

A. Oversight

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee for the Utility, which is hereby designated to be the Selectboard. The Selectboard 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 to an appropriate degree 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.

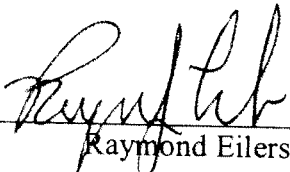
C. Service Provider Arrangements

In the event the Utility engages a service provider to perform an activity in connection with one or more accounts, the Utility will take reasonable steps toward ensuring that the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft. Such steps may, but are not required to, include:

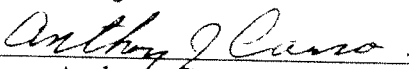
1. Requiring that service providers have such policies and procedures in place; and
2. Requiring that service providers review the Utility's Program and report any Red Flags to the Program Administrator.

The foregoing Policy is hereby adopted by the Selectboard of the Town of Readsboro of Readsboro, Vermont, this day of April 8, 2009, and is effective as of this date until amended or repealed.

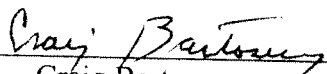
Signatures of the Selectboard:



Raymond Eilers, Chairperson



Anthony Caruso



Craig Bartosewcz

