POLICY #38

Town of Hopkinton, NH
Water/Sewer Departments

Identity Theft Prevention Program

Effective beginning June 1, 2010

Summary

I. PROGRAM ADOPTION

The Town of Hopkinton, NH Water/Sewer Departments ("Water/Sewer") 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 Board of Selectmen. After consideration of the size and complexity of the Water/Sewer's operations and account systems, and the nature and scope of the Water/Sewer's activities, the Board of Selectmen determined that this Program was appropriate for the Town of Hopkinton, NH Water/Sewer Departments, and therefore approved this Program on June 1, 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, a municipal Water or Sewer Department is a creditor subject to the Rule requirements. The Rule defines creditors "to include finance companies, automobile dealers, mortgage brokers, Water or Sewer Departments, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."

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

1. Any account the Water or Sewer Department that offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. Any other account the Water or Sewer Department offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Water or Sewer Department 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 Water or Sewer Department 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 Water or Sewer Department 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
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 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
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); and
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 holder is repeatedly returned as undeliverable;
5. Notice to the Water/Sewer that a customer is not receiving mail sent by the Water/Sewer;
6. Notice to the Water/Sewer that an account has unauthorized activity;
7. Breach in the Water/Sewer's computer system security; and
8. Unauthorized access to or use of customer account information.

E. Alerts from Others

Red Flag

1. Notice to the Water or Sewer Department 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 for a **new account**, Water/Sewer 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.

B. Existing Accounts

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

Detect

4. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
5. Verify the validity of requests to change billing addresses; and
6. Verify changes in banking information given for billing and payment purposes.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Water/Sewer 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

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 Town 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 Water/Sewer accounts, the Water/Sewer 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 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. Request only the last 4 digits of social security numbers (if any);
6. Ensure computer virus protection is up to date; and
7. Require and keep only the kinds of customer information that are necessary for Water/Sewer purposes.

VI. PROGRAM UPDATES

The Town Administrator will periodically review and update this Program to reflect changes in risks to customers and the soundness of the Water/Sewer from Identity Theft. In doing so, the Town Administrator will consider the Water/Sewer's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the Water/Sewer's business arrangements with other entities. After considering these factors, the Town Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Town Administrator will update the Program or present the Water/Sewer Department OR Board of Selectmen with his or her recommended changes and the Water/Sewer Department OR Board of Selectmen 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 Water/Sewer Departments. The Committee is headed by a Town Administrator who may be the head of the Water/Sewer Department or his or her appointee. Two or more other individuals appointed by the head of the Water/Sewer or the Town Administrator comprise the remainder of the committee membership. The Town Administrator will be responsible for the Program administration, for ensuring appropriate training of Water/Sewer 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

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

C. Service Provider Arrangements

In the event the Water/Sewer engages a service provider to perform an activity in connection with one or more accounts, the Water/Sewer 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 Water/Sewer's Program and report any Red Flags to the Town 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 the information those documents contain are considered "security information" as defined in Minnesota Statutes Section 13.37 and are unavailable to the public because disclosure of them would be likely to substantially jeopardized the security of information against improper use, that use being to circumvent the Water/Sewer's Identity Theft prevention efforts in order to facilitate the commission of Identity Theft.

_____
Christopher Lawless, Selectmen

_____
George A. Langwasser, Selectmen

_____
Tom Congoran, Selectmen

_____
Bryan Pellerin, Selectmen

_____
James O'Brien, Selectmen