TOWN OF FALMOUTH
MUNICIPAL SEWER THE DEPARTMENT

IDENTITY THEFT PREVENTION PROGRAM

Effective November 1, 2009

I. PROGRAM ADOPTION

The Town of Falmouth Water Pollution Control Department (the "Department") developed this Identity Theft Prevention Program (the "Program") pursuant to the Federal Trade Commission's Red Flags Rule (the "Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed with oversight and approval of the Town Manager and the Town Council. After consideration of the size and complexity of the Department's operations and account systems, and the nature and scope of the Department's activities, the Town Council determined that this Program was appropriate for the Town of Falmouth Water Pollution Control Department, and therefore approved and adopted this Program on October 26, 2009.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

The purpose of the Program is to comply with the 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. The 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. Findings

1. The Department is a creditor pursuant to 16 CFR § 681.2 due to its provision of covered accounts for which payment is made in arrears.
2. Covered accounts offered to customers for the provision of services include wastewater accounts.
3. The Department does not accept Debit or Credit Cards for payment, but its service provider may. The Department does not require customers to provide social security numbers.

4. The Department has had no previous experience with identity theft related to covered accounts.
5. The processes of opening a new covered account, restoring an existing covered account, maintaining account information and making payments on such accounts have been identified as potential processes in which identity theft could occur.
6. The Department has engaged the Portland Water District as its exclusive service provider for all activity on wastewater accounts.
7. The Department offers covered accounts, but does not create or maintain covered accounts onsite. The Department is provided with monthly reports from its service provider.
8. The Department determines that there is a *low* risk of identity theft occurring in the following ways*:*
    a. Use by an applicant of another person's personal identifying information to establish a new covered account; ***low***
    b. Use of a previous customer's personal identifying information by another person in an effort to have service restored in the previous customer's name; ***low***
    c. Use of another person's credit card, bank account, or other method of payment by a customer to pay such customer's covered account or accounts; ***None, so long as neither the Department nor the Service Provider accepts credit or debit cards or processes ACH transactions.***
    d. Use by a customer desiring to restore such customer's covered account of another person's credit card, bank account, or other method of payment; ***None, so long as neither the Department nor the Service Provider accepts credit or debit cards or processes ACH transactions.***

C. Red Flags Rule definitions used in this Program

For purposes of this Program the following definitions apply:

Identity theft means fraud committed using the identifying information of another person.

Identifying information means 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.

Red Flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

According to the Rule, a municipal utility is a creditor subject to the Rule requirements. The Rule defines creditors "to include finance companies, automobile dealers, mortgage brokers, the Department companies, and telecommunications companies. Where non-profit and

government entities defer payment for goods or services, they, too, are to be considered creditors."

All Departments accounts that are individual utility service accounts held by customers of the Department whether residential, commercial or industrial are covered by the Rule. A **covered account** is:

1. Any account the Department offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. Any other account the Department offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Department from identity theft.

Service provider means a person or business entity that provides a service directly to the Department relating to or in connection with a covered account. With respect to sewer services, the Department has engaged the Portland Water District, a public municipal corporation with a principal place of business at 225 Douglas Street, Portland, Maine, as its exclusive service provider for the creation of, access to and maintenance of covered accounts (the "Service Provider").

III. CREATION OF AND ACCESS TO COVERED ACCOUNTS

Service Provider shall be responsible for creation of and access to covered accounts.

IV. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the 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. Since the Service Provider is responsible for the process of opening a covered account, restoring a covered account or accepting payment for a covered account, it shall also be responsible to check for Red Flags as indicators of possible identity theft. Such Red Flags may include the following:

A. 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 inconsistent with the person presenting the document;
3. Other document with information that is inconsistent with existing customer information (such as if a person's signature on a check appears forged or name on credit card does not match customer name).

B. 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 consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
3. A person fails to provide complete personal identifying information on an application when requested to do so. (By law, social security numbers must not be required); and
4. A person's identifying information is inconsistent with the information that is on file for the customer.

C. Alerts from Others

Red Flag

1. Notice to the Department from a customer, identity theft victim, law enforcement, Service Provider or other person that it has opened or is maintaining a fraudulent account for a person engaged in identity theft.

V. 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,** the Identity Theft Prevention Program that Service Provider follows shall include, at a minimum, 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, telephone number, 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. Independently contact the customer.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an **existing account,** the Identity Theft Prevention Program that Service Provider follows shall include, at a minimum, 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 or credit card given for billing and payment purposes.

C. Processing Payments

In order to detect any of the Red Flags identified above associated with **payment on an account,** the Identity Theft Prevention Program that Service Provider follows shall include, at a minimum, the following steps to obtain and verify the identity of the person opening the account:

Detect

1. Cross-check with the financial institution any banking information provided for electronic payments, unless a voided check or deposit slip with customer's name is provided.
2. Require any service provider processing credit card payments over the Internet to certify that it has in place an adequate identity theft prevention program applicable to such payments.

VI. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Service Provider detects any identified Red Flags, the Identity Theft Prevention Program that it follows shall take one or more of the following steps, or reasonably similar 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. Not open a new account;
4. Close an existing account;
5. Reopen an account with a new number;
6. Refuse to accept payment on the account;
7. Notify law enforcement in instances of suspected or confirmed identity theft.

Protect customer identifying information

In order to further prevent the likelihood of identity theft occurring with respect to the Department accounts, the Service Provider's Identity Theft Prevention Program shall require it to take the following steps, or reasonably similar steps, with respect to its internal operating procedures to protect the Department's 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. Ensure computer virus protection is up to date;
6. Require and keep only the customer information that is necessary for the Department account purposes.
7. Do not print the entire credit or debit card or bank account number used for payment of the covered account on any account statements or receipts.

VII. PROGRAM UPDATES

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the Department from identity theft. At least every year, the Program Administrator will consider the Department's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the Department maintains and changes in the Department's business arrangements with service providers. 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.

VIII. PROGRAM ADMINISTRATION

A. Oversight

The Superintendant of the Department shall be designated as the Program Administrator. The Program Administrator will be responsible for: (i) the Program administration; (ii) reviewing Service Provider's Identity Theft Protection Program submitted to the Department for compliance with the Rule with respect to services performed for the Department; Iiii) reviewing any reports from Service Provider regarding the detection of Red Flags and the steps for preventing and mitigating identity theft; (iv) determining which steps of prevention and mitigation should be taken in particular circumstances; and (v) considering periodic changes to the Program.

B. Staff Training

Service Provider staff responsible for implementing its Program shall be trained by Service Provider in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. The Department shall give Service Provider staff instruction on the requirement and procedure to report certain incidents of possible identity theft to the Department.

C. Service Provider Arrangements

The Department has engaged Service Provider to perform all activities in connection with covered accounts. The Department shall take the following steps to ensure that Service Provider performs its activities in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

The Department shall require by contract that Service Provider shall:

1. Acknowledge receipt and review of this Program, or in the alternative, deliver a copy of its own Identity Theft Protection Program to the Department for review and acceptance by the Department;
2. Agree to perform its services in compliance with the terms and conditions of this Program or the Service Provider's Program, if accepted by the Department;
3. Take appropriate actions to prevent and mitigate identity theft;
4. Report promptly to the Department in writing if Service Provider, in connection with its services for the Department, detects an incident of actual or attempted identity theft or is unable to resolve one or more Red Flags that Service Provider detects in connection with a covered account.