

*Agenda Item IV C*

**Valerie Capels**

**From:** Abigail Friedman [afriedman@vlct.org]  
**Sent:** Monday, May 04, 2009 4:13 PM  
**To:** Abigail Friedman  
**Cc:** Garrett Baxter  
**Subject:** Red Flags Rule - FTC Delays Enforcement

**Red Flags Rule**  
***Federal Trade Commission Delays Enforcement, Again***

On April 30<sup>th</sup>, the Federal Trade Commission (FTC) issued a press release announcing that it will yet again delay enforcement of the "Red Flags Rule".

The Red Flags Rule is part of the federal Fair and Accurate Credit Transactions (FACT) Act of 2003 under which creditors with covered accounts must develop and implement identity theft prevention programs to identify, detect and respond to potential indicators or "red flags" of identity theft. The FTC previously confirmed that the Red Flags Rule applies to all municipal utilities and other operations such as municipal housing authorities that extend credit as part of a continuing relationship for services.

Affected municipalities now have until **August 1, 2009** to develop and implement a theft identity prevention program. The FTC also announced that it will soon release a template for entities that have a low risk of identity theft. The FTC's latest press release can be accessed online at <http://www.ftc.gov/opa/2009/04/redflagsrule.shtm>. The **VLCT Model Identity Theft Prevention Policy** and the **VLCT Identity Theft Prevention Memo of April 14** are also available online. For more information contact Garrett Baxter, VLCT Staff Attorney, at 1-800-649-7915 or [gbaxter@vlct.org](mailto:gbaxter@vlct.org).

Sincerely,  
**Abigail Friedman**  
Director, Municipal Assistance Center  
Vermont League of Cities and Towns  
89 Main Street, Suite 4  
Montpelier, VT 05602

800-649-7915  
T: 802-229-9111  
F: 802-229-2211

## Valerie Capels

**From:** Garrett Baxter [gbaxter@vlct.org]  
**Sent:** Tuesday, April 14, 2009 4:02 PM  
**To:** Garrett Baxter  
**Subject:** Re: Identity Theft Red Flags rule

Dear Municipal Officials,

On March 20<sup>th</sup>, the VLCT Municipal Assistance Center released a model identity theft prevention policy to assist municipalities in complying with the Federal Trade Commission's (FTC) Identity Theft Red Flags rule which was promulgated in furtherance of the federal Fair and Accurate Credit Transactions Act (FACTA). Since that time, we have received numerous questions, both regarding the federal regulation and the model policy itself.

### ***Who must comply with the Red Flags rule?***

Any municipality (town, city, village, fire or water district, solid waste district, and all other governmental entities) operating a utility, acting as a financial institution or creditor, or providing services prior to billing. Municipalities with compliance question should consult the Federal Trade Commission's (FTC) article: The "Red Flags" Rule: Are You Complying with New Requirements for Fighting Identity Theft?  
<http://www.ftc.gov/bcp/edu/pubs/articles/art10.shtm>

### ***Does the Identity Theft Red Flags rule apply to the collection of property taxes?***

No. FTC staff counsel has confirmed that the rule only applies to those municipalities that extend "credit" for the provision of services. Property taxes are considered "involuntary payments" and as such do not fall under the definition of "credit" under the rule.

### ***Our municipality only collects names and addresses. Does the Red Flags rule still apply?***

The answer to this question is unclear, but Senior Legislative Counsel at the National League of Cities believes that it does. Accordingly, we suggest that so long as any personal information is collected, even if it is just names and addresses, that some type of identity theft prevention policy, regardless of how sparse, be implemented.

### ***Our municipality does not believe that the Red Flags rule applies. What should we do?***

The FTC's red flag rules state that every covered creditor must periodically conduct a risk assessment to determine whether it offers or maintains covered accounts by taking into consideration the methods it uses to open accounts, access accounts and its previous experiences with identity theft. If a municipality believes that the Red Flags rule does not apply, it should state as much on the record during the course of an open meeting. This could be accomplished by having the legislative body ask of itself, its town manager/administrator, finance officer, municipal clerk or treasurer whether it meets the FTC's definition of a "financial institution" or "creditor" and whether it offers or maintains "covered accounts" (see definitions below). If the answer to these questions is "no", then the chair of the legislative body should move that after conducting a risk assessment and determining that the Red Flags rule does not apply, the municipality will not implement a written Identity Theft Prevention Program. The minutes should reflect that the legislative body or town manager considered the application of the Identity Theft Red Flags rule and determined it was not applicable. Because the Red Flags rule requires municipalities to periodically determine the applicability of the rule, we recommend that this risk assessment be performed on an annual basis.

### ***Much of VLCT's model policy does not appear to apply to us. Does our municipality have to adopt the entirety of VLCT's model policy as written?***

No. As stated above, the first step in complying with the Identity Theft Red Flags rule is for a municipality's legislative body to conduct a risk assessment to determine whether the municipality offers or maintains "covered accounts". This should be done taking into consideration the methods it provides to open its accounts, the methods it provides to access its accounts, and its experiences with identity theft. Municipalities that fall under the Red Flags rule must then develop and implement a Theft Identity Prevention Program that includes "reasonable policies and procedures to:

1. Identity relevant Red Flags for the covered accounts that the financial

5/26/2009

5/26/2009

- institution or creditor offers or maintains, and incorporate those Red Flags into its Program;
2. Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;
  3. Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and
  4. Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft."

VLCT's model Identity Theft Prevention Policy reflects these four mandatory provisions of the Program (see Sections 3-6 of the model policy). While a municipality's Program must include policies and procedures to accomplish these four tasks, how it does so is left entirely up to the municipality. The policies and procedures included under the model policy's section headings are merely guidelines, i.e. suggestions that were included to assist in the formulation of a policy that fulfills the requirements of the law. Although municipalities must take these suggestions into consideration, they are in no way obligated to adopt them. Municipalities are free to tailor their Programs to incorporate the guidelines they find are appropriate to their size, complexity and the nature and scope of their activities.

Again, municipalities should convene a meeting of its legislative body and ask of itself, its town manager/administrator, finance officer, municipal clerk or treasurer, and determine which sections of the required provisions (Sections 3-6 of the model policy) are applicable. It may well be that many of the sections are not applicable, resulting in the adoption of a scaled down, bare bones policy. Such a policy is in keeping with the requirements of the law, so long as the minutes reflect that the municipality's legislative body or manager conducted a risk assessment that considered the risk that identity theft poses to its covered accounts and adopted a policy appropriate for its size, complexity and nature of its operations.

As always, please feel free to call or email us with any questions.

Sincerely,

*Garrett A. Baxter*

Garrett A. Baxter, Esq.  
Staff Attorney, Municipal Assistance Center  
Vermont League of Cities and Towns  
1-800-649-7915  
[gbaxter@vlct.org](mailto:gbaxter@vlct.org)

The information contained in this transmission may contain privileged and confidential information. It is intended only for the use of the person(s) to whom it is addressed above. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution or duplication of this communication is prohibited. If you are not the intended recipient, please contact the sender by reply email or telephone and destroy all copies of the original message. Thank you.

5/26/2009



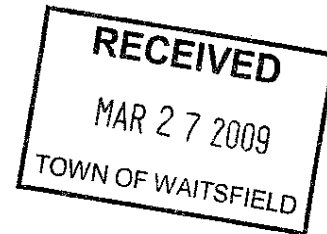
89 Main Street, Suite 4  
Montpelier, Vermont  
05602-2948

Tel.: (802) 229-9111  
Fax: (802) 229-2211

e-mail:  
info@vlct.org

web:  
www.vlct.org

## MEMORANDUM



**To:** Municipal Officials

**From:** Abigail Friedman, Director, and  
Garrett Baxter, Staff Attorney  
VLCT Municipal Assistance Center

**Date:** March 20, 2009

**RE:** Identity Theft Prevention Policy

---

The VLCT Municipal Assistance Center has developed the attached model identity theft policy to assist municipalities in developing and implementing a theft identity prevention program.

Final rules known as "Red Flag" rules, adopted by the Federal Trade Commission (FTC) under direction of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), require all creditors with covered accounts to implement an identity theft prevention program by May 1, 2009. The FTC has confirmed that these rules apply to all municipalities (town, city, village, fire or water district, solid waste district, and all other governmental entities) operating a utility (water, sewer, electric, gas, telecommunications, etc.) and any other municipal operations extending credit (i.e., defer payment) for services (possible examples include housing authorities and recreation departments).

In order to come into compliance with these federal regulations, municipalities should conduct an assessment of their existing policies, procedures, and other arrangements to control reasonably foreseeable risks to customers from identity theft. Each municipality will have to work closely with its attorney and those department heads, managers, elected and appointed officials, and staff responsible for processing covered accounts to ensure compliance and proper administration and oversight of the program.

Recognizing that the direction and control of municipal utilities differ from municipalities around the state provides the option of vesting the authority and responsibility for the adoption, administration, and oversight of the identity theft prevention program in either the Legislative Body (Selectboard, Board of Trustees, City Council, Prudential Committee), Board of Water Commissioners, Board of Sewage System Commissioners, Board of Sewage Disposal Commissioners, and/or Board of Electric Commissioners, as appropriate. Regardless of the arrangement, this policy requires that municipal utilities make annual reports to the Legislative Body and that such a policy governing the operations of each and every municipal utility be in place by May 1, 2009.

*Sponsor of:*

VLCT Health Trust, Inc.

VLCT Municipal Assistance  
Center

VLCT Property and Casualty  
Intermunicipal Fund, Inc.

VLCT Unemployment  
Insurance Trust, Inc.

As always, please feel free to call us with any questions.

# Identity Theft Prevention Policy

## [Municipality] of \_\_\_\_\_, Vermont

### Section 1: Title, Authority, and Purpose

This policy shall be known as the “[Municipality] of \_\_\_\_\_ Identity Theft Prevention Policy.” It has been adopted by the [Municipality] of \_\_\_\_\_ [Selectboard pursuant to 24 V.S.A. §§ 872, 1121 and 1122 or other Legislative Body, e.g. trustees, prudential committee, etc., pursuant to their respective statutory authority.] **OR** [Board of Water Commissioners pursuant to 24 V.S.A. § 3313(a)] **OR** [Board of Sewage System Commissioners pursuant to 24 V.S.A. § 3507] **OR** [Board of Sewage Disposal Commissioners pursuant to 24 V.S.A. § 3616(a)] **OR** [Board of Electric Commissioners pursuant to 30 V.S.A. § 2915].

The purpose of this Policy is to establish an Identity Theft Prevention Program (“Program”) designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair Accurate Credit Transactions Act (FACTA) of 2003.

### Section 2: Definitions

For the purposes of this Policy, the following definitions apply:

**Covered Account** means:

- an account that a creditor offers or maintains – primarily for personal, family, or household purposes – that involves or is designed to permit multiple payments or transactions, such as an utility account; and
- any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

**Credit** means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor.

**Creditor** means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. Creditor includes any municipal utility (water, sewer, electric, etc.).

**Customer** means a person that has a covered account with a creditor.

**Department Personnel** means all employees responsible for or involved in the process of opening a covered account, restoring a covered account, or accepting payment for a covered account.

**Identity theft** means a fraud committed or attempted using the identifying information of another person without authority.

**Person** means a natural person, a corporation, government or governmental subdivision, or agency, trust, estate, partnership, cooperative, or association.

- The Social Security Number (SSN) has not been issued or is listed on the Social Security Administrator's Death Master File.
  - Personal identifying information provided by the customer is inconsistent with other personal identifying information provided by the customer, such as a lack of correlation between the SSN range and date of birth.
  - Personal identifying information or a phone number or address is associated with known fraudulent activities as indicated by internal or third-party sources used by the department.
  - Personal identifying information, such as a fictitious mailing address, mail drop address, jail address, invalid phone number, pager number, or answering service, is associated with fraudulent activities as indicated by internal or third-party sources used by the creditor.
  - The SSN provided is the same as that submitted by another applicant or customer.
  - The address or telephone number provided is the same as or similar to the covered account number or telephone number submitted by an unusually large number of applicants or customers.
  - The applicant or customer fails to provide all required personal identifying information on an application or in response to the notification that the application is incomplete.
  - Personal identifying information is inconsistent with personal identifying information on file with the department.
  - The applicant or customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
- **Unusual Use of or Suspicious Activity Related to the Covered Account**
    - Shortly following the notice of a change of address for a covered account, the department receives a request for the addition of authorized users on the account.
    - A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example:
      - The customer fails to make the first payment, or makes an initial payment but no subsequent payments.
    - A covered account is used in a manner inconsistent with established patterns of activity on the account. For example:
      - Nonpayment when there is no history of late or missed payments, or
      - A material increase in the use of available credit.
    - A covered account that has been inactive for a reasonably lengthy period of time is used.
    - Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
    - The department is notified that the customer is not receiving paper account statements.
    - The department is notified of unauthorized charges or transactions in connection with the customer's account.

- **Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Creditor.**
  - The department is notified by a customer, a victim of identity theft, law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

#### **Section 4: Detecting Red Flags**

- **New Covered Accounts**  
In order to detect any of the red flags identified above associated with the opening of a new covered account, department personnel will take the following steps to obtain and verify the identity of the person opening the account:
  - Require submission of all of the following identifying information from the customer prior to opening a covered account:
    - name;
    - date of birth;
    - address, which shall be:
      - for an individual, a residential or business street address;
      - for an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, or the residential or business address of a next of kin of another contact individual;
      - for an entity, a principal place of business, local office or other physical address;
      - for a U.S. person, a taxpayer identification number;
      - for a non-U.S. person, one or more of the following:
        - a taxpayer identification number;
        - passport number and country of issuance;
        - alien identification card number; or
        - number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.
  - Verify the customer's identity (for instance, review a driver's license or other identification card);
  - Review documentation showing the existence of a business entity; and
  - Independently contact the customer.
- **Existing Accounts**  
In order to detect any of the red flags identified above for an existing covered account, department personnel will take the following steps to monitor transactions with an account:
  - Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email, etc.);
  - Monitor transactions;
  - Verify the validity of change of address requests and other account information requests including information provided for billing and payment purposes.

## Section 5: Preventing and Mitigating Identity Theft

If department personnel detect any identified red flags, such personnel, after consultation with his/her program administrator, shall take one or more of the following appropriate responses commensurate with the degree of risk posed by the red flag in order to further prevent the likelihood of identity theft occurring with respect to covered accounts:

- Continuing to monitor a covered account for evidence of identity theft;
- Contacting the customer;
- Changing any passwords, security codes, or other security devices that permit access to covered accounts;
- Not opening a new covered account;
- Closing an existing covered account;
- Reopening a covered account with a new account number;
- Not attempting to collect on a covered account;
- Not selling a covered account to a debt collector;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances.

## Section 6: Program Updates

The [Legislative Body] OR [Board of Water Commissioners] OR [Board of Sewage System Commissioners] OR [Board of Sewage Disposal Commissioners] OR [Board of Electric Commissioners] shall annually review and, as it deems necessary, update this program along with any relevant red flags to reflect changes in risks to customers or to the safety and soundness of the department from identity theft based on the following factors:

- The department's experiences with identity theft;
- Changes in methods of identity theft;
- Changes in identity theft detection, prevention, and mitigation methods;
- Changes in the types of accounts that the department offers or maintains; and
- Changes in the department's business arrangements with other entities.

## Section 7: Program Administration

- **Oversight:** The [Legislative Body] OR [Board of Water Commissioners] OR [Board of Sewage System Commissioners] OR [Board of Sewage Disposal Commissioners] OR [Board of Electric Commissioners] shall be responsible for the oversight of the program including program implementation, reviewing reports prepared by staff regarding the detection, prevention, and mitigation of identity theft in connection with the opening of a covered account or an existing covered account, and approving material changes to the program as necessary to address changing identity theft risks.
- **Staff Reports:** Department staff responsible for implementing the program shall report to the [Legislative Body] and the [Board of Water Commissioners] OR [Board of Sewage System Commissioners] OR [Board of Sewage Disposal Commissioners] OR [Board of Electric

Commissioners] annually on compliance with red flag requirements. The report will address material matters related to the program and evaluate issues such as:

- The effectiveness of the policies and procedures of the department in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
  - Service provider arrangements;
  - Significant incidents involving identity theft and management's response; and
  - Recommendations for material changes to the program.
- **Staff Training:** The [Legislative Body] **OR** [Board of Water Commissioners] **OR** [Board of Sewage System Commissioners] **OR** [Board of Sewage Disposal Commissioners] **OR** [Board of Electric Commissioners] **OR** its authorized representative will train staff responsible for effectively implementing the program as necessary.
  - **Oversight of Service Provider Arrangements:** If the [Legislative Body] **OR** [Board of Water Commissioners] **OR** [Board of Sewage System Commissioners] **OR** [Board of Sewage Disposal Commissioners] **OR** [Board of Electric Commissioners] engages a service provider to perform an activity in connection with one or more covered accounts, the [Legislative Body] **OR** [Board of Water Commissioners] **OR** [Board of Sewage System Commissioners] **OR** [Board of Sewage Disposal Commissioners] **OR** [Board of Electric Commissioners] will review such arrangements in order to ensure that the service provider's activities are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

The foregoing Policy is hereby adopted by the [Legislative Body] **OR** [Board of Water Commissioners] **OR** [Board of Sewage System Commissioners] **OR** [Board of Sewage Disposal Commissioners] **OR** [Board of Electric Commissioners] of the [Municipality] of \_\_\_\_\_, Vermont, this day of \_\_\_\_\_ and is effective as of this date until amended or repealed.

**Signatures of [Legislative Body] **OR** [Board of Water Commissioners] **OR** [Board of Sewage System Commissioners] **OR** [Board of Sewage Disposal Commissioners] **OR** [Board of Electric Commissioners]:**

\_\_\_\_\_  
Chairperson  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_