Identity Theft Prevention Policy
Town of Fair Haven, Vermont

Section 1: Title, Authority, and Purpose

This policy shall be known as the "Town of Fair Haven Identity Theft Prevention Policy." It has been adopted by the Town of Fair Haven, 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.

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.
Personal Identifying Information means a person's credit card account information, debit card information, bank account information, and driver's license information, and for a natural person includes his or her social security number, mother's birth name, and date of birth.
Red flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Section 3: Identification of Relevant Red Flags

In order to identify relevant red flags, the Selectboard 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 Selectboard identifies the following examples of relevant red flags, in each of the listed categories:

- **Alerts, Notifications, or Warnings from Consumer Reporting Agencies**
  - A fraud or active duty alert that is included with a consumer report.
  - A notice of credit freeze in response to a request for a consumer report.
  - A notice of address discrepancy provided by a consumer reporting agency.
  - A consumer report indicating a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
    - A recent and significant increase in the volume of inquiries;
    - An unusual number of recently established credit relationships;
    - A material change in the use of credit, especially with respect to recently established credit relationships; or
    - An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

- **Suspicious Documents**
  - Documents provided for identification that appear to have been altered or forged.
  - Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer presenting the identification.
  - Other information on the identification that is inconsistent with information provided by the person opening a new covered account or a customer presenting the information.
  - Other information on the identification that is inconsistent with readily accessible information that is on file with the department, such as a signature card or a recent check.
  - An application that appears to have been altered, forged, destroyed, or reassembled.

- **Suspicious Personal Identifying Information**
  - Personal identifying information presented that is inconsistent with external information sources used by the department. For example:
    - The address does not match any address in the consumer reports; or
    - 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 Selectboard 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 Selectboard 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 Selectboard 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 Selectboard its authorized representative will train staff responsible for effectively implementing the program as necessary.

- **Oversight of Service Provider Arrangements:** If the Selectboard engages a service provider to perform an activity in connection with one or more covered accounts, the Selectboard 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 Selectboard of the Town of Fair Haven, Vermont, this day of 4/7/09 and is effective as of this date until amended or repealed.

Signatures of Selectboard:

Ron Adams, Chairmen

Julie Ellis

Raymond Bunker

Jeff Sheldon

Claire Stanley