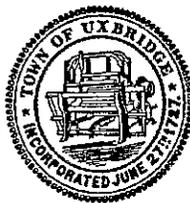


Adopted by BOS  
6/14/10



## Red Flag Policy and Identity Theft Prevention Program

### Purpose

To establish an Identity Theft Prevention 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 and Accurate Credit Transactions Act (FACTA) of 2003.

### Definitions

1. **Covered Account** means:
  - a. An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, tax bill, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and
  - b. Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.
2. **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 therefore.
3. **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 and includes utility companies and telecommunications companies.
4. **Customer** means a person that has a covered account with a creditor.
5. **Identity theft** means a fraud committed or attempted using identifying information of another person without authority.
6. **Notice of address discrepancy** means a notice sent to a user by a consumer reporting agency pursuant to 1 U.S.C. § 1681 (c)(h)(1)

7. **Person** means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.
8. **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 their social security number, mother's birth name, and date of birth.
9. **Red flag** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
10. **Service provider** means a person that provides a service directly to the Town.
11. **Town** means the Town of Uxbridge.

### **Findings**

1. The Town is a creditor pursuant to 16 CFR § 681.2 due to its provision or maintenance of covered accounts for which payment is made in arrears.
2. Covered accounts offered to customers for the provision of Town services include utility accounts and development review accounts.
3. The process of opening a new covered account and making payments on such accounts have been identified as potential processes in which identity theft could occur.
4. The Town limits access to personal identifying information to those employees responsible for or otherwise involved in opening covered accounts or accepting payment for use of covered accounts. Information provided to such employees is entered directly into the Town's computer system and is not otherwise recorded.
5. The Town determines that there is a low risk of identity theft occurring in the following ways:
  - Use by an applicant of another person's personal identifying information to establish a new covered account; and
  - 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.

### **Process of Establishing a Covered Account**

As a precondition to opening a covered account in the Town, each applicant shall provide the Town with a valid government issued identification card containing a photograph of the applicant. The identifying number of card shall be recorded on the application for service.

### **Access to Covered Account Information**

1. Access to customer accounts shall be password protected and shall be limited to authorized Town personnel.
2. Any unauthorized access to or other breach of customer accounts is to be reported immediately to the Town Manager.
3. Personal identifying information included in customer accounts is considered confidential and any request or demand for such information shall be immediately forwarded to the Finance Director.

### **Credit Card Payments**

In the event that credit card payments that are made over the Internet are processed through a third party service provider, such third party service provider shall certify that it has an adequate identity theft prevention program in place that is applicable to such payments.

### **Sources and Types of Red Flags**

All employees responsible for or involved in the process of opening a covered account or accepting payment for a covered account shall check for red flags as indicators of possible identity theft and such red flags may include:

1. Alerts from consumer reporting agencies, fraud detection agencies or service providers. Examples of alerts include but are not limited to:
  - A fraud or active duty alert that is included with a consumer report;
  - A notice of a credit freeze in response to a request for a consumer report;
  - A notice of address discrepancy provided by a consumer reporting agency;
  - Indications of a pattern of activity in a consumer report 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;
    - ❖ A material change in the use of credit, especially with respect 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.

2. Suspicious documents. Examples of suspicious documents include:

- Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer;
- Documents provided for identification that appeared to be altered or forged;
- Identification on which the information is inconsistent with information provided by the applicant or customer;
- Identification on which the information is inconsistent with readily accessible information that is on file with the creditor, such as the application for service; or
- An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.

3. Suspicious personal identification, such as suspicious address change. Examples of suspicious identifying information include:

- Personal identifying information that is inconsistent with external information sources used by the financial institution or creditor. For example:
  - ❖ The address does not match any address in the consumer report;
  - ❖ The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
- Personal identifying information provided by the customer is not consistent 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 applications or activities as indicated by internal or third-party sources used by the financial institution or creditor.
- Other information provided, such as fictitious mailing address, mail drop addresses, jail addresses, invalid phone numbers, pager numbers or answering services, is associated with fraudulent activity.
- The SSN provided is the same as that submitted by other applicants or customers.
- The address or telephone number provided is the same as or similar to the 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 notification that the application is incomplete.
- Personal identifying information is not consistent with personal identifying information that is on file with the financial institution or creditor.
- The applicant or customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

4. Unusual use of or suspicious activity relating to a covered account. Examples of suspicious activity include:
- Shortly following the notice of a change of address for an account, Town 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 patterns. For example:
    - ❖ The customer fails to make the first payment or makes an initial payment but no subsequent payments.
  - An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
    - ❖ Nonpayment when there is no history of late or missed payments.
    - ❖ A material change in purchasing or spending patterns;
  - An account that has been inactive for a long period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
  - Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.
  - The Town is notified that the customer is not receiving paper account statements.
  - The Town is notified of unauthorized charges or transactions in connection with a customer's account.
  - The Town is notified by a customer, law enforcement or another person that it has opened a fraudulent account for a person engaged in identity theft.
5. Notice from customers, law enforcement, victims or other reliable sources regarding possible identity theft or phishing relating to covered accounts.

### **Prevention and Mitigation of Identity Theft**

In the event that any Town employee responsible for or involved in restoring an existing covered account or accepting payment for a covered account becomes aware of red flags indicating possible identity theft with respect to existing covered accounts, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the Town Manager. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to the Town Manager, who may in his or her discretion determine that no further action is necessary. If the Town Manager in his or her discretion determines that further action is necessary, a Town employee shall perform one or more of the following responses, as determined to be appropriate by the Town Manager:

- Contact the customer;
  - Make the following changes to the account if, after contacting the customer, apparent that someone other than the customer has accessed the customer's covered account:
    - ❖ change any account numbers, passwords, security codes, or other security devices that permit access to a account; or
    - ❖ close the account;
  - Cease attempts to collect additional charges from the customer and decline to sell the customer's account to a debt collector in the event that the customer's account has been accessed without authorization and such access has caused additional charges to accrue;
  - Notify a debt collector within [select time frame, for example, 48 hours] of the discovery of likely or probable identity theft relating to a customer account that has been sold to such debt collector in the event that a customer's account has been sold to a debt collector prior to the discovery of the likelihood or probability of identity theft relating to such account;
  - Notify law enforcement, in the event that someone other than the customer has accessed the customer's account causing additional charges to accrue or accessing personal identifying information; or
  - Take other appropriate action to prevent or mitigate identity theft.
2. In the event that any Town employee responsible for or involved in opening a new covered account becomes aware of red flags indicating possible identity theft with respect an application for a new account, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the Town Manager. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to the Town Manager, who may in his or her discretion determine that no further action is necessary. If the Town Manager in his or her discretion determines that further action is necessary, a Town employee shall perform one or more of the following responses, as determined to be appropriate by the Town Manager:

- Request additional identifying information from the applicant;
- Deny the application for the new account;
- Notify law enforcement of possible identity theft; or
- Take other appropriate action to prevent or mitigate identity theft.

## Updating the Program

The Board of Selectmen shall periodically review and, as deemed necessary by the Board of Selectmen update the Identity Theft Prevention Program along with any relevant red flags in order to reflect changes in risks to customers or to the safety and soundness of the Town and its covered accounts from identity theft. In so doing, the Board of Selectmen shall consider the following factors and exercise its discretion in amending the program:

- The Town's experiences with identity theft;
- Updates in methods of identity theft;
- Updates in customary methods used to detect, prevent, and mitigate identity theft;
- Updates in the types of accounts that the Town offers or maintains; and
- Updates in service provider arrangements.

### **Program Administration**

The Town Manager is responsible for oversight of the program and for program implementation, and is responsible for reviewing reports prepared by staff regarding compliance with red flag requirements and with recommending material changes to the program, as necessary in the opinion of the Town Manager, to address changing identity theft risks and to identify new or discontinued types of covered accounts. Any recommended material changes to the program shall be submitted to the Board of Selectmen for their consideration.

1. The Finance Director will report to the Town Manager at least annually, on compliance with the red flag requirements. The report will address material matters related to the program and evaluate issues such as:
  - a. The effectiveness of the policies and procedures of Town in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
  - b. Service provider arrangements;
  - c. Significant incidents involving identity theft and management's response; and
  - d. Recommendations for material changes to the Program.
  
2. The Finance Director is responsible for providing training to all employees responsible for or involved in opening a new covered account or accepting payment for a covered account with respect to the implementation and requirements of the Identity Theft Prevention Program. The Finance Director shall exercise his or her discretion in determining the amount and substance of training necessary.

### **Outside Service Providers**

In the event that the Town engages a service provider to perform an activity in connection with one or more covered accounts the Finance Director shall exercise his or her discretion in reviewing such arrangements in order to ensure, to the best of his or her ability, that the service provider's activities are conducted in accordance with policies and procedures, agreed upon by contract, that are designed to detect any red flags that may arise in the performance of the service provider's activities and take appropriate steps to prevent or mitigate identity theft.

## **Treatment of Address Discrepancies**

Pursuant to 16 CFR § 681.1, this establishes a process by which the Town will be able to form a reasonable belief that a consumer report relates to the consumer about whom it has requested a consumer credit report when the Town has received a notice of address discrepancy. In the event the Town receives a notice of address discrepancy, the Town employee responsible for verifying consumer addresses for the purpose of providing the municipal service or account sought by the consumer shall perform one or more of the following activities, as determined to be appropriate by such employee:

1. Compare the information in the consumer report with:
  - a. Information the Town obtains and uses to verify a consumer's identity in accordance with the requirements of the Customer Information Program rules implementing 31 U.S.C. § 5318(1);
  - b. Information the Town maintains in its own records, such as applications for service, change of address notices, other customer account records or tax records; or
  - c. Information the Town obtains from third-party sources that are deemed reliable by the relevant Town employee; or
2. Verify the information in the consumer report with the consumer.

## **Furnishing Consumer's Address to Consumer Reporting Agency**

1. In the event that the Town reasonably confirms that an address provided by a consumer to the Town is accurate, the Town is required to provide such address to the consumer reporting agency from which the Town received a notice of address discrepancy with respect to such consumer. This information is required to be provided to the consumer reporting agency when:
  - a. The Town is able to form a reasonable belief that the consumer report relates to the consumer about whom the Town requested the report;
  - b. The Town establishes a continuing relation with the consumer; and
  - c. The Town regularly and in the ordinary course of business provides information to the consumer reporting agency from which it received the notice of address discrepancy.
2. Such information shall be provided to the consumer reporting agency as part of the information regularly provided by the Town to such agency for the reporting period in which the Town establishes a relationship with the customer.

## Methods of Confirming Consumer Addresses

The Town employee charged with confirming consumer addresses may, in his or her discretion, confirm the accuracy of an address through one or more of the following methods:

1. Verifying the address with the consumer;
2. Reviewing the Town's records to verify the consumer's address;
3. Verifying the address through third party sources; or
4. Using other reasonable processes.

Policy adopted administratively by the Town Manager as of 06/01/2010

Michael A. Szlosek Michael Szlosek, Town Manager

6/1/2010 Date

Policy reviewed and adopted by the Board of Selectmen on 06/14/10

