TITLE XVIII: IDENTITY THEFT PREVENTION PROGRAM

Chapter

18.01. IDENTITY THEFT PREVENTION PROGRAM

Chapter 18.01: IDENTITY THEFT PREVENTION PROGRAM

Added 10-16-08

SECTION

General Provisions

General Provisions

§ 18.01.001 Program Adoption

This Identity Theft Prevention Program ("Program") is adopted 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.

§18.01.002 Definitions

(A) “Covered Account” means and refers to (i) 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, mortgage loan, automobile loan, margin account, cell phone account, checking account, or savings account; and (ii) 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.

(B) “Customer” means and refers to a person that has a covered account with the Town.

(C) “Identifying information” shall be as defined under the Rule, as amended from time to time. As of the effective date of this Ordinance, it means “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” and shall include: 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.

(D) "Identity Theft" means and refers to fraud committed using the identifying information of another person.

(E) "Person" means and refers to a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

(F) "Program Administrator" shall mean and refer to that person designated by the Town Council for the administration and enforcement of this Ordinance, or his designee.

(G) "Red Flag" means and refers to a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

(H) "Town" means and refers to the Town of River Bend.

(I) "Utility" shall mean and refer to any board, commission, district, department, provider or other agency or department of Town that provides any type of public utility service, or which is otherwise subject to the Rule.

§18.03.003 Identification of Red Flags

In order to identify relevant Red Flags, the Utility 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 Utility identifies the following red flags, in each of the listed categories:

(A) Notifications and Warnings From Credit Reporting Agencies

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

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

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

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 Utility that a customer is not receiving mail sent by the Utility;
6. Notice to the Utility that an account has unauthorized activity;
7. Breach in the Utility's computer system security; and
8. Unauthorized access to or use of customer account information.

(E) Alerts from Others

1. Notice to the Utility 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.

§18.01.004 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, Utility personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, residential or business address, 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 photo identification card);
3. Review documentation showing the existence of a business entity; and

4. Independently contact the customer.

(B) Existing Accounts

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

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.

§18.01.005 Preventing and Mitigating Identity Theft

In the event Utility 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:

(A) Prevention and Mitigation

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 Program 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.

(B) Protect customer identifying information

In order to further prevent the likelihood of identity theft occurring with respect to Utility accounts, the Utility will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. If applicable, 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;
7. Access to customer accounts shall be limited to Town personnel only; and
8. Require and keep only the kinds of customer information that are necessary for utility purposes.

§18.01.006 Program Updates

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the Utility from Identity Theft. At least once per year, the Program Administrator will consider the Utility's experiences with Identity Theft situation, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the Utility maintains and changes in the Utility's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. Thereafter, he shall update the Town Council with his recommended changes, if any, and the Town Council will make a determination of whether to make any changes to the Program.

§18.01.007 Program Administration

(A) Oversight

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee for the Utility. The Committee is headed by a Program Administrator who may be the head of the Utility or his or her appointee. Two or more other individuals appointed by the head of the Utility or the Program Administrator comprise the remainder of the committee membership. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of Utility 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

Utility staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. The Utility should include in its Program how often training is to occur. Staff shall provide reports to the Program Administrator on incidents of Identity Theft, the Utility's compliance with the Program and the effectiveness of the Program at least annually.

The reports should address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the creditor 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.

(C) Service Provider Arrangements

In the event the Utility engages a service provider to perform an activity in connection with one or more accounts, the Utility 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 Utility's Program and report any Red Flags to the Program Administrator.

(D) Specific Program Elements and Confidentiality

For the effectiveness of Identity Theft prevention Programs, the Red Flag Rule envisions a degree of confidentiality regarding the Utility's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices are to be limited to the Identity Theft Committee and those employees who need to know them for purposes of preventing Identity Theft. Because this Program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program's general red flag detection, implementation and prevention practices are listed in this document.

§18.01.008 Severability; Conflict with Other Laws

(A) Severability

If any section, clause or provision of this Ordinance shall be found to be invalid, the validity of the remaining sections, clauses or provisions shall not be affected thereby.

(B) Conflict with Other Laws

Whenever the regulations of this ordinance conflict with the requirements of another statute, the more restrictive standard shall apply.

§ 18.01.009 Effective Date

This Ordinance shall become effective immediately upon adoption.