



City of Wyoming, Michigan
Administrative Policy

Subject: Identity Theft Prevention Program

Department: Andrea Boot, Treasurer

Department Head: /s/Andrea Boot

Date: 10/24/2008

Curtis Holt, City Manager: /s/Curtis Holt

Date: 10/27/2008

[Original policy October 2008.]

This page was intentionally left blank.

IDENTITY THEFT PREVENTION PROGRAM

I. OBJECTIVE

The purpose of this Identity Theft Prevention Program (Program) is to protect customers of the City of Wyoming's utility services from identity theft. The Program is designed to comply with the Federal Trade Commission's (FTC) Identity Theft Red Flag Rule and is intended to establish reasonable policies and procedures to facilitate the detection, prevention and mitigation of identity theft in connection with the opening of new Covered Accounts and activity on existing Covered Accounts.

II. SCOPE

All utilities are required to comply with the FTC's "Identity Theft Fed Flag Rule" even if only nominal information such as name, phone number and address are collected. This Program applies to the creation, modification and access to Identifying Information of a customer of the utilities operated by the Municipality (water and sewer) by any and all personnel of the Municipality, including management personnel. The primary purpose of the rule is to protect against the establishment of false accounts and ensure existing accounts are not being manipulated. This regulation does not address or require utilities to adopt measures that will protect consumer information and prevent unauthorized access. Although the true risk established through the risk assessment activity may not require any changes to existing policies or procedures, implementation of good management practices to protect personal consumer data can prevent identity theft. This Program does not replace or repeal any previously existing policies or programs addressing some or all of the activities that are the subject of this Program, but rather it is intended to supplement any such existing policies and programs.

III. DEFINITIONS

When used in this Program, the following terms have the meanings set forth opposite their name, unless the context clearly requires that the term be given a different meaning:

Creditor: 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, utility companies, and telecommunication companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors." (16 CFR 681.2(b)(5).

Covered Account: The term "covered account" means an account that the City of Wyoming offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments of transactions. (16 CFR 681.2(b)(3)(i)). A utility account is a "covered account." The term "covered account" also includes other accounts offered or maintained by the Municipality for which there is

a reasonably foreseeable risk to customers the Municipality or its customers from identity theft. (16 CFR 681.2(b)(3)(ii)).

Identity Theft: The term “identity theft” means a fraud committed or attempted using the identifying information of another person without authority. (16 CFR §681.2(b)(8) and 16 CFR §603.2(a)).

Identifying Information: The term “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 any name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. Additional examples of “identifying information” are set forth in 16 CFR §603.2(a).

Red Flag: The term “Red Flag” means a pattern, practice or specific activity that indicates the possible existence of identity theft.

Certain terms used but not otherwise defined herein shall have the meanings given to them in the FTC’s Identity Theft Rules (16 CFR Part 681) or the Fair Credit Reporting Act of 1970 (15 U.S.C. §1681 *et seq.*), as amended by the Fair and Accurate Credit Transactions Act of 2003 into law on December 4, 2003. (Public Law 108-159).

IV. POLICY

Administration of the Program

This Program is intended to identify red flags that will alert employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, methods to ensure existing accounts were not opened using false information, and measures to respond to such events.

The Senior Management Person responsible for this program is:

City Treasurer

Phone number: (616) 530-7282

Identity Theft Prevention Elements

Identification of Relevant Red Flags

The City of Wyoming has considered the guidelines and the illustrative examples of possible Red Flags from the FTC’s Identity Theft Rules and has reviewed the Municipality’s past history with instances of identity theft, if any. The municipality

hereby determines that the following are the relevant Red Flags for purposes of this Program given the relative size of the Municipality and the limited nature and scope of the services that the Municipality provides to its citizens:

A. The presentation of suspicious documents.

1. Documents provided for identification appear to have been altered or forged.
2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
3. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
4. Customer fails to provide all information requested.

B. The presentation of suspicious personal identifying information, such as a suspicious address change.

1. Personal information provided is inconsistent with information on file for a customer.
2. Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet.

C. Notice of Possible Identity Theft.

1. The Municipality is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

Detection of Red Flags

The employees of the City of Wyoming that interact directly with customers on a day-to-day basis shall have the initial responsibility for monitoring the information and documentation provided by the customer and any third-party service provider in connection with the opening of new accounts and the modification of or access to existing accounts and the detection of any Red Flags that might arise. Management shall see to it that all employees who might be called upon to assist a customer with the opening of a new account or with modifying or otherwise accessing an existing account are properly trained such that they have a working familiarity with the relevant Red Flags identified in this Program so as to be able to recognize any Red Flags that might surface in connection with the transaction. An Employee who is not sufficiently trained to recognize the Red Flags identified in this Program shall not open a new account for any customer, modify any existing account or otherwise provide any customer with access to information in an existing account without the direct supervision and specific approval of a management employee. Management employees shall be properly trained such that

they can recognize the relevant Red Flags identified in this Program and exercise sound judgment in connection with the response to any unresolved Red Flags that may present themselves in connection with the opening of a new account or with modifying or accessing of an existing account. Management employees shall be responsible for making the final decision on any such unresolved Red Flags.

Response to Detected Red Flags

Any employee of the City of Wyoming that may suspect fraud or detect a Red Flag will implement the following response as applicable. All detections or suspicious Red Flags shall be reported to the Treasurer.

1. Ask the applicant for additional documents.
2. Contact the customer (existing accounts).
3. Notify internal manager: Any utility employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customer's identity must notify the Treasurer or Deputy Treasurer
4. Notify law enforcement: The Treasurer or Deputy Treasurer or designee will notify the City of Wyoming Police Department of any attempted or actual identity thefts.
5. Do not open the account.
6. Close the account.

V. PROGRAM MANAGEMENT AND ACCOUNTABILITY

Initial Risk Assessment – Covered Accounts

Utility accounts for personal, family and household purposes are specifically included within the definition of “covered account” in the FTC’s Identity Theft Rules. Therefore, the City of Wyoming determines that with respect to its residential utility accounts it offers and/or maintains covered accounts. The Municipality also performed an initial risk assessment to determine whether the utility offers or maintains any other accounts for which there are reasonably foreseeable risks to customers or the utility from identity theft. In making this determination the Municipality considered (1) the methods it uses to open its accounts, (2) the methods it uses to access its accounts, and (3) its previous experience with identity theft, and it concluded that it does not offer or maintain any such other covered accounts.

Program Updates – Risk Assessment

The Program, including relevant Red Flags, is to be reviewed as often as necessary but at least annually to reflect changes in risks to customers from Identity Theft. Factors to consider in the Program update include:

1. An assessment of the risk factors identified above.
2. Any identified Red Flag weaknesses in associated account systems or procedures.

3. Changes in methods of Identity Theft.
4. Changes in methods to detect, prevent, and mitigate Identity Theft.
5. Changes in business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

Training and Oversight

All city staff performing any activity in connection with one or more Covered Accounts are to be provided appropriate training and receive effective oversight to ensure that the activity is conducted in accordance with policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

For the effectiveness of Identity Theft prevention programs, the Red Flag Rule envisions a degree of confidentiality regarding the City'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 Program Administrator, appropriate senior management staff and those employees who need to know them for purpose of preventing Identity Theft. Because this Program will be 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.

VI. RESPONSIBILITY

The initial adoption and approval of the Identity Theft Prevention Program shall be by administrative policy approved by the City Manager. Thereafter, changes to the Program of a day-to-day operational character and decisions relating to the interpretation and implementation of the Program may be made by the Treasurer (Program Administrator). Major changes or shifts of policy positions under the Program shall be approved by the City Manager.

Development, implementation, administration and oversight of the Program will be the responsibility of the Program Administrator. The Program Administrator may, but shall not be required to, appoint a committee to administer the Program. The Program Administrator shall be the head of any such committee. The Program Administrator will report at least annually to the City Manager regarding compliance with this Program.

Issues to be addressed in the annual Identity Theft Prevention Report include:

1. The effectiveness of the policies and procedures in addressing the risk of Identity Theft in connection with the opening of new Covered Accounts and activity with respect to existing Covered Accounts.
2. Significant incidents involving Identity Theft and management's response (if any).
3. Recommendations for material changes to the Program, if needed for improvement.