

## **Title 1: Program Adoption**

The City of Hewitt Water and Wastewater Utility, hereinafter Utility or Utilities, developed this Identity Theft Prevention Program, hereinafter “program” pursuant to the Federal Trade Commission’s Red Flag Rule, hereinafter “rule”, which implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003. 16 C. F. R §681.2. This program was developed with oversight of the City of Hewitt Utility Committee, consisting of Mayor Luke Mitchell, Council Member Johannes Marsland, Utility Maintenance Supervisor Blayne Brisson and City Clerk/Treasurer Miriam A. Collom, and with approval of the City of Hewitt City Council. After consideration of the size and complexity of the Utility’s operations and account systems, and the nature and scope of the Utility’s activities, the Utility Committee and the City Council of the City of Hewitt determined that this program was appropriate for the City of Hewitt Water and Wastewater Utilities, and therefore approved this program on (date).

## **Title 2: Program Purpose and Definitions**

### **Part 1: Fulfilling the requirements of the Red Flag Rule**

Under the Red Flag Rule, every financial institution and creditor is required to establish an “Identity Theft Prevention Program” tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4. Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor to Identity Theft.

### **Part 2: Red Flag Rules definitions used in this Program**

Identity Theft: Fraud committed using the identity information of another person

Red Flag: A pattern, practice or specific activity that indicates the possible existence of Identity Theft

Creditor: The Rule defines creditors “to include finance companies, automobile dealers, mortgage brokers and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors.

Covered Account: a) any account the Utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and  
b) any other account the Utility offers or maintains for which there is a reasonably foreseeable risk to the customers or to the safety and soundness of the Utility from Identity Theft.

Identifying Information: any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including name, address, telephone number(s), social security number, date of birth, government issued driver’s license, government issued identification number, alien registration number, unique electronic identification number, computer’s Internet Protocol address or routing code.

## **Title 3: 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 offers

to access its accounts, and its previous experience with Identity Theft. The Utility identifies the following Red Flags, in each of the listed categories:

**A) Notifications and Warnings From Credit Reporting Agencies**

*Red Flags:*

- 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**

*Red Flags:*

- 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; and
- 4) Application for service that appears to have been forged or altered.

**C) Suspicious Personal Identifying Information**

*Red Flags:*

- 1) Identifying information that is inconsistent with other information the customer provides;
- 2) Identifying information presented that is inconsistent with other sources of information;
- 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 other fraudulent activity
- 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 who fails to provide complete personal identifying information on an application when reminded to do so; and
- 8) A person's identifying information is not consistent with the information that is on file with the customer.

**D) Suspicious Account Activity or Unusual Use of Account**

*Red Flags:*

- 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;
- 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**

*Red Flags:*

- 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.

#### **Title 4: Detecting Red Flags**

##### **Part 1: 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 that may include, but is not limited to, name, date of birth, residential or business address, principal place of business, driver's license or other identification;
- 2) Verify the customer's identity;
- 3) Review documentation showing the existence of a business entity; and
- 4) Independently contact the customer.

##### **Part 2: Existing Accounts**

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

- 1) Verify the identification of customers if they request information;
- 2) Verify the validity of requests to change billing addresses; and
- 3) Verify changes in banking information given for billing and payment purposes.

#### **Title 5: 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 identified Red Flag:

- 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 steps to take;
- 8) Notify Law Enforcement; and/or
- 9) Determine that no response is warranted under the particular circumstances.

#### **Title 6: 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 annually, the City of Hewitt Utility Committee will consider the Utility's experiences with Identity Theft situations, 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 City of Hewitt Utility Committee will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the City of Hewitt Utility Committee will update the Program or present the City of Hewitt City Council with his or her recommended changes and the City of Hewitt City Council will make a determination of whether to accept, modify or reject those changes to the Program.

#### **Title 7: Program Administration**

##### **Part 1: Oversight**

Responsibility for developing, implementing and updating this Program lies within an Identity Theft Committee for the Utility. The Committee is 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 circumstance and considering periodic changes to the Program.

### **Part 2: Staff Training and Reports**

Utility staff responsible for implementing the Program shall be trained under the direction of the City of Hewitt Utility Committee in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

### **Part 3: Service Provider Arrangements**

In the event the Utility engages in 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 City of Hewitt Utility Committee.

### **Part 4: 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 City of Hewitt Utility 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.