

City of West University Place
Harris County, Texas

RESOLUTION NO. 2009-05

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF WEST UNIVERSITY PLACE, TEXAS, ADOPTING A WRITTEN IDENTITY THEFT PROGRAM POLICY AND AUTHORIZING THE CITY MANAGER TO APPROVE CHANGES IN THE POLICY.

WHEREAS, Federal Trade Commission (FTC) adopted rules on identity theft “red flags”, or warning signs, pursuant to the Fair and Accurate Credit Transactions (FACT) Act of 2003; and

WHEREAS, the new rules, which require action by May 1, 2009, require any business with a “covered account” to implement an identity theft program; and

WHEREAS, a city with such accounts must adopt a program by May 1, 2009 that “red flags” relevant identity theft, provides detection of the “red flags”, provides appropriate responses for any “red flags” detected, and ensures the program is updated periodically to address changing risks; and

WHEREAS, the City of West University Place services such water utility customers and, therefore falls within this federal mandate; and

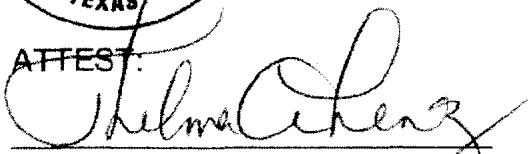
WHEREAS, the City Council of the City of West University Place wishes to be proactive and adopt an Identity Theft Program Policy that will be in compliance with the criteria set forth by the FTC.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF WEST UNIVERSITY PLACE, to adopt the Identity Theft Program/Policy that is in compliance with federal law and is attached to this resolution as Exhibit “A”.

This resolution shall be effective immediately upon its adoption on this ^{13th} ~~25th~~ day of



ATTEST:


Thelma Lenz, City Secretary

APPROVED:


Bob Kelly, Mayor



CITY OF WEST UNIVERSITY PLACE

Identity Theft Program/Policy

I. PROGRAM ADOPTION

The City of West University Place ("City") developed this Identity Theft Prevention Program ("Program") 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. This Program was developed for the Utility Department of the City ("Utility") with oversight and approval of the Finance Director and the 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 Finance Director and the City Council determined that this Program was appropriate for the City of West University Place, and therefore approved this Program at the regular council meeting held on March 23, 2009.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling Requirements of the Red Flags 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 from Identity Theft.

B. Red Flags Rule definitions used in this Program

1. **City:** The City of West University Place, Texas.
2. **Covered Account:** Any account the Utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and any other account the Utility offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Utility from Identity Theft. All the Utility's accounts that are individual utility service accounts held by customers of the utility whether residential, commercial or industrial are covered by the Rule.
3. **Creditors:** Includes finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors. According to the Rule, a municipal utility is a creditor subject to the Rule requirements.
4. **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, 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.

C. Application

This policy applies to all City employees and service providers that have access to the utility customer's personal information that is submitted, regardless of the medium (i.e., in person, by email, by fax, through regular mail or over the internet).

III. 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. 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 (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.

B. 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 (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.

C. Alerts from Others

Red Flag

1. Notice to the Utility from a customer, identity theft victim, fraud detection service, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

IV. DETECTING RED FLAGS.

A. Detection of 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 identification card);
3. Review documentation showing the existence of a business entity; and
4. Independently contact the customer or business.

B. Detection of 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 close accounts or change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

V. 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:

Prevent and Mitigate

1. Continue to monitor an account for evidence of Identity Theft;

2. Contact the customer, sometimes through multiple methods;
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 Finance Director 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.

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. 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 according to State record retention laws;
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. Ensure computer virus protection is up to date; and
6. Require and keep only the kinds of customer information that are necessary for utility purposes.

VI. 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 Finance Director 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, consult with law enforcement authorities, and consult with other City personnel. After considering these factors, the Finance Director will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Finance Director will update the Program or present the City Council with his or her recommended changes and the City Council will make a determination of whether to accept, modify or reject those changes to the Program.

VII. PROGRAM ADMINISTRATION.

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the Finance Director. The Finance Director 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. Service Provider Arrangements

In the event the Utility engages a service provider to perform an activity in connection with one or more accounts, including but not limited to franchise utility providers, 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 or contract amendment, that service providers have such policies and procedures in place; and
2. Require, by contract or contract amendment, that service providers review the Utility's Program and report any Red Flags to the Finance Director.

C. Specific Program Elements and Confidentiality

For the effectiveness of this Identity Theft prevention program, knowledge of such specific practices is to be limited to the Finance Director and those employees who need to know them for purposes of preventing Identity Theft. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered "security information" and are unavailable to the public because disclosure of them would likely substantially jeopardized the security of information against improper use, that use being to circumvent the Utility's Identity Theft prevention efforts in order to facilitate the commission of Identity Theft.