

ORDER ESTABLISHING IDENTITY THEFT PREVENTION PROGRAM

April 1, 2009

THE STATE OF TEXAS §
 §
COUNTY OF TRAVIS §

WHEREAS, Travis County Municipal Utility District No. 2 (the "District") is a political subdivision of the State of Texas, created and operating under Chapters 49 and 54 of the *Texas Water Code*;

WHEREAS, in accordance with the Fair and Accurate Credit Transactions Act of 2003 (Public Law 108-159), the Federal Trade Commission has promulgated identity theft regulations set forth in Title 16, Part 681 of the Code of Federal Regulations (the "Red Flags Regulations") which require a government or governmental subdivision to implement an identity theft prevention program to protect accounts offered or maintained primarily for personal, family or household purposes that involve or are designed to permit multiple payments or transactions, including utility accounts, and any other accounts that are offered or maintained for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the government or governmental subdivision from identity theft, including financial, operational, compliance, reputation or litigation risks;

WHEREAS, the District maintains or may maintain in the future customer accounts for utility services and/or other purposes that are or may become subject to the Red Flag Regulations;

WHEREAS, in order to comply with the Red Flags Regulations and in an effort to detect, prevent, and mitigate identity theft in connection with any customer accounts of the District, the Board of Directors of the District (the "Board") desires to adopt an identity theft prevention program;

IT IS, THEREFORE, ORDERED BY THE BOARD OF DIRECTORS OF TRAVIS COUNTY MUNICIPAL UTILITY DISTRICT NO. 2 that:

Section 1: Upon considering the size and complexity of the District's operations and account systems and the nature and scope of the District's activities, the Board has designed the Identity Theft Prevention Program (the "Program") attached as Exhibit "A", which is hereby adopted.

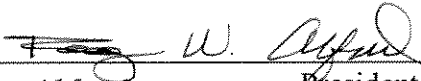
Section 2: The Program will be reviewed and updated periodically, as necessary, to reflect changes in risks to the District's customers and the safety and soundness of the District from identity theft.

Section 3: If the application of any provision of this Order or the Program to any person or set of circumstances is for any reason held to be unconstitutional, invalid, or unenforceable, the validity and applicability of the remaining portions of this Order and the Program will not be affected, it being the intent of the Board, in adopting this Order and the

Program, that no provision of this Order or the Program will become inoperative or fail by reason of the unconstitutionality or invalidity of any other provision.

PASSED AND APPROVED this 1st day of April, 2009.

**TRAVIS COUNTY MUNICIPAL UTILITY
DISTRICT NO. 2**

By: 
Roger Alford, President
Board of Directors

ATTEST:

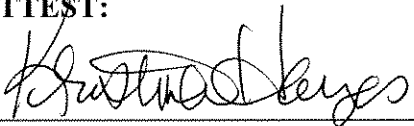

Kristina Hayes, Secretary
Board of Directors

EXHIBIT "A"

IDENTITY THEFT PREVENTION PROGRAM

I. *Approval of the Program.*

The Board of Directors (the "Board") of Travis County Municipal Utility District No. 2 (the "District") hereby establishes the following Identity Theft Prevention Program (the "Program") and commits to implementing this Program according to the procedures set forth below.

II. *Definitions.*

A. "**Account**" means a continuing relationship established by a person or entity with the District to obtain a product or service for personal, family, household or business purposes.

B. "**Covered Account**" means any Account which the District maintains or may maintain in the future, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions and any other Account that the District maintains or may maintain in the future for which there is a reasonably foreseeable risk to Customers or to the safety and soundness of the District from Identity Theft, including financial, operational, compliance, reputation or litigation risks.

C. "**Customer**" means a person or entity with a Covered Account.

D. "**Identifying Information**" means any name or number that may be used, along or in conjunction with any other information, to identify a specific person.

E. "**Identity Theft**" means an actual or attempted fraud committed by using the Identifying Information of another person without authority.

F. "**Red Flag**" means patterns, practices or specific activities that indicate the possible existence of Identity Theft associated with one or more Covered Accounts.

G. "**Service Provider**" means a person or entity engaged by the District to perform an activity in connection with one or more Covered Accounts.

III. *Purpose.*

A. The purpose of this Program is to identify and detect Red Flags and establish procedures for preventing and mitigating the risk of Identity Theft.

IV. *Risk Assessment.*

A. The District conducted an internal risk assessment to evaluate the procedures for opening and accessing Covered Accounts in order to determine whether Covered Accounts could be susceptible to Identity Theft. Using this information, the District identified the following Red Flags:

1. presentation of suspicious documents, including:
 - a. documents that appeared to have been altered or forged;
 - b. documents that contain information inconsistent with information on file or other information provided by a person opening a new Covered Account; and
 - c. photo identification that is inconsistent with the appearance of the person opening a new Covered Account;
2. presentation of Identifying Information that is:
 - a. inconsistent with information on file, other information provided by a person opening a new Covered Account or information obtained through an external source;
 - b. similar or identical to information, particularly addresses and phone numbers, provided on fraudulent applications or agreements;
 - c. is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources (for example, the address on an application is fictitious, a mail drop, or a prison or the phone number is invalid or associated with a pager or answering service);
 - d. is the same information provided for another Covered Account or Covered Accounts; and
 - e. does not include all required information, even after notification;
3. unusual use or suspicious activity related to a Covered Account, including:
 - a. a request to add one or more authorized persons to an existing Covered Account, particularly if the additional persons have different last names than the primary Customer;
 - b. a significant spike in water usage on a Covered Account;
 - c. a material change in electronic fund transfer patterns in connection with a deposit account;
 - d. inactivity associated with a Covered Account for a reasonably lengthy period of time;
 - e. repeated problems with mail sent to a Customer (e.g. mail is repeatedly returned as undeliverable despite water usage remaining at normal levels);
 - f. notifications to the District that a Customer is not receiving paper account statements; and

g. notifications to the District of unauthorized charges or transactions in connection with a Covered Account; and

4. notice received from Customers, law enforcement or others of possible or actual Identity Theft or any other unusual activity related to a Covered Account (for example, notification that the District has opened a fraudulent account for a person engaged in Identity Theft).

V. *Detection.*

A. The District will endeavor to detect Red Flags by implementing one or more the following procedures in connection with Covered Accounts:

1. obtaining the following identifying information from a new Customer:

- a. name;
- b. date of birth;
- c. address; and

d. identification number, which shall be, for a U.S. person, a taxpayer identification number, and for a non-U.S. person, one or more of the following: a taxpayer identification number; passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard;

2. verifying customer information through documentation, including unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and

3. verifying the validity of change of address requests for existing Covered Accounts.

VI. *Response.*

A. Upon detecting a Red Flag, the District will take the appropriate action, which may include:

- 1. monitoring a Covered Account where there is suspicion of Identity Theft;
- 2. contacting all affected Customers;
- 3. changing any passwords, security codes, or other security devices that permit access to a Covered Account;

4. closing the existing Covered Account and reopening it only after assigning it a new account number;

5. declining to open a new Covered Account;
6. closing an existing Covered Account;
7. postponing attempts to collect on a Covered Account;
8. notifying law enforcement; or
9. determining that no response is warranted under the particular circumstances.

VII. Administration, Oversight and Training.

A. The Board will oversee the development, implementation and administration of the Program. If the District has engaged a Service Provider to manage the billing and collecting aspects of certain Covered Accounts, that Service Provider will administer this Program in terms of detecting, preventing and mitigating Identity Theft with respect to those Covered Accounts.

B. The District will require that all activities of a Service Provider related to a Covered Account are conducted in accordance with this Program and the Service Provider's internal policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft. A Board-appointed subcommittee may from time to time inspect a Service Provider's policies and procedures for detecting, preventing and mitigating the risk of Identity Theft to ensure that they are reasonable and effective.

C. The District will provide this Program, and updates to this Program, to a Service Provider to ensure that this Program is properly implemented.

D. The District will require any staff of the District that is responsible for development, implementation and administration of this Program or a Service Provider, if appropriate, to present to the Board, at least annually and in a format and manner reasonably designed to protect the security of the District and Customers, a report addressing material matters related to this Program and evaluating issues such as:

1. the effectiveness of policies and procedures of the District and, if appropriate, the Service Provider in addressing the risk of Identity Theft in connection with Covered Accounts;
2. significant incidents of Identity Theft related to one or more Customers and the response to such incidents; and
3. recommendations for material changes to this Program, including new methods and technologies available for detecting Identity Theft.

E. The Board will periodically review and, if appropriate, update this Program to reflect changes in risks to Customers and the safety and soundness of the District from Identity Theft.

F. The District will require that any employees, contractors, and agents who open, access, service or handle Covered Accounts be trained to effectively implement this Program.