RESOLUTION ESTABLISHING AN IDENTITY THEFT PREVENTION PROGRAM

THE STATE OF TEXAS §
COUNTY OF HARRIS §
FAULKEY GULLY MUNICIPAL UTILITY DISTRICT §

WHEREAS, pursuant to the Red Flags Rule (Section 114 of the Fair and Accurate Credit Transactions Act of 2003), the Federal Trade Commission adopted rules pertaining to identity theft prevention ("Identity Theft Rules"); and

WHEREAS, the Identity Theft Rules require creditors to adopt an Identity Theft Prevention Program on or before May 1, 2009; and

WHEREAS, the Red Flags Rule defines "creditor" to include all utility companies; and

WHEREAS, Faulkey Gully Municipal Utility District (the "District") provides utility services and accepts payments for services and is therefore classified as a "creditor" under the Identity Theft Rules; and

WHEREAS, the Board of Directors of the District desires to develop the Identity Theft Prevention Program (the "Program") set forth in Exhibit "A," attached hereto and incorporated herein for all purposes; and

WHEREAS, the Board of Directors of the District has reviewed the Program and believes it fulfills, complies with, and implements the Red Flags Rule and other requirements outlined by the Federal Trade Commission; and

WHEREAS, the Board of Directors of the District finds that it is in the public interest to approve the Program.

NOW, THEREFORE, BE IT RESOLVED BY THE BOARD OF DIRECTORS OF FAULKEY GULLY MUNICIPAL UTILITY DISTRICT OF HARRIS COUNTY, TEXAS THAT:

Section 1. The foregoing recitals are hereby found to be true and correct and are hereby adopted by the Board of Directors of the District and made a part hereof for all purposes as findings of fact.

Section 2. All procedures and requirements of the Identity Theft Prevention Program shall be implemented as outlined in the Exhibit "A."

Section 3. This Resolution shall take effect immediately from and after its adoption.

Section 4: The President or Vice President and Secretary or Assistant Secretary of the Board of Directors are authorized and directed to do any and all things necessary and proper in connection with this application.

PASSED AND APPROVED on this 16th day of April, 2009.

By: /s/ Kenneth R. Kana
President, Board of Directors

ATTEST:

By: /s/ Alexander W. Schultz
Secretary, Board of Directors

(DISTRICT SEAL)

# Faulkey Gully
# Municipal Utility District

# Identity Theft Prevention Program

Effective beginning May 1, 2009

# IDENTITY THEFT PREVENTION PROGRAM

## I.

## PROGRAM ADOPTION

Faulkey Gully Municipal Utility District (the "District") hereby develops 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 with oversight and approval of the Program Administrator as defined below. After consideration of the size and complexity of the District's operations and account systems, and the nature and scope of the District's activities, the Program Administrator determined that this Program was appropriate for the District and therefore approved this Program on April 16, 2009.

## II.

## PROGRAM PURPOSE AND DEFINITIONS

### 2.1 Fulfilling Requirements of the Red Flags Rule

The District hereby establishes an "Identity Theft Prevention Program" to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
1. Detect Red Flags that have been incorporated into the Program;
2. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
3. 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.

### 2.2 Red Flags Rule Definitions used in this Program

"Identity Theft" is a fraud committed using the identifying information of another person.

"Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

"Creditors" are 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.

"Covered account" is:

1. Any account the District offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. Any other account the District offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the District from Identity Theft.

"Identifying information" is 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.

III.

## IDENTIFICATION OF RED FLAGS

In identifying Red Flags, the District has considered 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 District identifies the following red flags, in each of the listed categories:

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

E. Red Flags as to Alerts from Others

Notice to the District 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.

## IV.

## DETECTING RED FLAGS

### A. Detected Red Flags on New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new account, the following steps will be followed 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.

### B. Detected Red Flags on Existing Accounts

In order to detect any of the Red Flags identified above for an existing account, the following steps will be taken to monitor transactions of 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.

## V.

## PREVENTING AND MITIGATING IDENTITY THEFT

In the event District 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;
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.

VI.

## PROTECTING CUSTOMER IDENTIFYING INFORMATION

In order to further prevent the likelihood of Identity Theft occurring with respect to District accounts, the following steps will be taken with respect to protecting customer identifying information:

1. Ensure that websites are 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; and
7. Require and keep only the kinds of customer information that are necessary for District purposes.

VII.

## PROGRAM UPDATES

The Program Administrator, as hereinafter defined, will periodically review and update this Program to reflect changes in risks to customers and the soundness of the District from Identity Theft. The Program will be reviewed and updated at least once annually. As part of the review, the Operator and Tax Assessor/Collector will provide the Board of Directors with information about any experiences with Identity Theft situations, changes in Identity Theft methods, and changes in Identity Theft detection and prevention methods. The Board of Directors will also consider changes in the District's business arrangements with other entities. After considering these factors, the Board of Directors, as Program Administrator, will determine whether changes to the Program, including the listing of Red Flags, are warranted.

VIII.

## PROGRAM ADMINISTRATION

### A. Oversight

The District shall cause this Identity Theft Program to be implemented by the District's Operator and Tax Assessor/Collector. The Board of Directors of the District shall be considered the Program Administrator.

### B. Staff Training and Reports

The District's Operator and Tax Assessor/Collector shall be responsible for implementing this Identity Theft Program and training their personnel in the detection of Red Flags and in the responsive steps to be taken when a Red Flag is detected.

### C. Service Provider Arrangements

The Operator and Tax Assessor/Collector for the District shall each provide to the District either (1) a certification substantially in the form set forth as Exhibit "A," attached hereto, as to the receipt of this Identity Theft Program and the implementation of the procedures and controls set forth in this Identity Theft Program in their normal business operations, including procedures for training personnel in the Identity Theft Program; or (2) a certification substantially in the form set forth in Exhibit "B," attached hereto, stating that the company has implemented an Identity Theft Program that fulfills the requirements of the District's Program and establishes controls in normal business operations to ensure compliance with the Identity Theft Program, including procedures for training personnel.

### D. Non-disclosure of Specific Practices

For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices must be limited to the District and its identified consultants. 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 "exceptions" as defined in Sections Chapter 552, Texas Government Code, and are unavailable to the public as disclosure of them would likely jeopardize the security of information against improper use, that use being to circumvent the District's Identity Theft prevention efforts in order to facilitate the commission of Identity Theft.

EXHIBIT "A"

CERTIFICATION OF RECEIPT
AND IMPLEMENTATION OF IDENTITY THEFT PREVENTION PROGRAM

THE STATE OF TEXAS §
§
COUNTY OF _____ §

I, _____ of _____ do hereby certify that I have been presented a copy of the IDENTITY THEFT PREVENTION PROGRAM (the "Identity Theft Program") for Faulkey Gully Municipal Utility District. I have thoroughly reviewed the Identity Theft Program. _____ has implemented in its normal business operations the procedures and controls set forth in the Identity Theft Program, including procedures for training personnel in the Identity Theft Program.

WITNESS MY HAND THIS _____ day of _____, 2009.

By: _____
Name: _____
Title: _____

EXHIBIT "B"

CERTIFICATION OF IMPLEMENTATION
OF IDENTITY THEFT PREVENTION PROGRAM

THE STATE OF TEXAS §
§
COUNTY OF _____ §

I, _____ of _____ do hereby certify that I have been presented a copy of the IDENTITY THEFT PREVENTION PROGRAM (the "Identity Theft Program") for Faulkey Gully Municipal Utility District. I have thoroughly reviewed the Identity Theft Program. _____ has implemented in its normal business operations procedures and controls that provide the security of accounts as required under the District's Identity Theft Program and under the Identity Theft Rules adopted by the Federal Trade Commission, including procedures for training personnel in procedures for preventing identity theft.

WITNESS MY HAND THIS _____ day of _____, 2009.

By: _____
Name: _____
Title: _____