1.0 Purpose and Need

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, 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:

a. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;

b. Detect Red Flags that have been incorporated into the Program;

c. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and

d. 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.

2.0 Definitions

"Covered Account" means any account HRSD offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and any other account HRSD offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of HRSD from Identity Theft. All of HRSD's accounts that are individual utility service accounts held by customers of HRSD whether residential, commercial or industrial are covered by the Rule.

"Creditor" as defined by the Rule includes finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Non-profit and government entities that defer payment for goods or services are also considered creditors.

"Identifying information" is defined under the Rule as 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.

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

"Program" means HRSD's Identify Theft Prevention Program.

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

"Rule" means the Federal Trade Commission's Red Flags Rule.

3.0 Guiding Principles

In the course of doing business, while billing and collecting fees for its services, HRSD stores and maintains customer account data. As part of its fiduciary responsibility in accordance with Section 114 of the Fair and Accurate Credit Transactions Act of 2003, 16 C. F. R. § 681.2, this Identity Theft Prevention Policy is being implemented.

4.0 Procedures

In order to identify relevant Red Flags, HRSD 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. HRSD identifies the following red flags, in each of the listed categories:

a. 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.

b. 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 the service address in HRSD's database);
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 information (other than social security number) on an application; and
8. A person's identifying information is not consistent with the information that is on file for the customer.

c. Suspicious Account Activity or Unusual Use of Account

1. Account used in a way that is not consistent with prior use (example: very high activity);
2. Mail sent to the account holder is repeatedly returned as undeliverable;
3. Notice to the Utility that a customer is not receiving mail sent by the Utility;
4. Notice to the Utility that an account has unauthorized activity;
5. Breach in the Utility's computer system security; and
6. Unauthorized access to or use of customer account information.

d. Alerts from Others - 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.

e. New Accounts - In order to detect any of the Red Flags identified above associated with the opening of a **new account**, HRSD 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.

f. Existing Accounts - In order to detect any of the Red Flags identified above for an **existing account**, HRSD 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 change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

g. Prevent and Mitigate - In the event HRSD 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:

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.

h. Protect customer identifying information - In order to further prevent the likelihood of Identity Theft occurring with respect to HRSD accounts, HRSD 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;
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 HRSD purposes; and
7. Ensure that only employees with a need to know have access to customer identifying information.

5.0 Responsibility and Authority

The Program Administrator will periodically review and update this Program to reflect changes in risks to customers and the soundness of HRSD from Identity Theft. In doing so, the Program Administrator will consider HRSD's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the Utility's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program or present Commission with their recommended changes and the Commission will make a determination of whether to accept, modify or reject those changes to the Program.

a. Oversight - Responsibility for developing, implementing and updating this Program lies with the Director of Information Services (DIS). The DIS will be responsible for the Program administration, for ensuring appropriate training of HRSD 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. Staff Training and Reports - HRSD staff responsible for implementing the Program shall be trained either by or under the direction of the DIS in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

c. Service Provider Arrangements - In the event HRSD engages a service provider to perform an activity in connection with one or more accounts, HRSD 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 Program and report any Red Flags to the Program Administrator.

Approved: R. Tyler Bland, III, Commission Chairman — 10/28/08 Date

Attest: Jennifer L. Heilman, Commission Secretary — 10/28/08 Date