APPENDIX F

IDENTITY THEFT PREVENTION PROGRAM

IDENTITY THEFT PREVENTION PROGRAM

I.   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" ("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.   Definitions

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

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

3.   "Identifying information" means 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.

4.   "District" means the Cedar Key Water and Sewer District.

II. IDENTIFICATION OF RED FLAGS.

A. Generally

In identifying relevant 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. Specific examples of Red Flags are set forth below for each of several different categories of Red Flags.

B. 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.

4. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

C. 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).

4. Application for service that appears to have been altered or forged.

D. 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.

8.   A person's identifying information is not consistent with the information that is on file for the customer.

E.   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.

8.   Unauthorized access to or use of customer account information.

F.   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.

III.   **DETECTING RED FLAGS.**

A.   **New Accounts**

In order to detect any of the Red Flags identified above associated with the opening of a new account, District personnel shall take the following steps to obtain and verify the identity of the person opening the account in one or more of the following ways:

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.

4.   Independently contact the customer.

B.   **Existing Accounts**

In order to detect any of the Red Flags identified above for an existing account, District 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.

3.   Verify changes in banking information given for billing and payment purposes.

IV.   **PREVENTING AND MITIGATING IDENTITY THEFT**

A.   **Mitigation**

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:

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 General Manager for determination of the appropriate step(s) to take.

8.   Notify law enforcement.

9.   Determine that no response is warranted under the particular circumstances.

B.   Prevention

In order to further prevent the likelihood of identity theft occurring with respect to District accounts, the District 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.   Request only the last 4 digits of social security numbers (if any).

6.   Ensure computer virus protection is up to date.

7.   Require and keep only the kinds of customer information that are necessary for utility purposes.

C.   **Program Updates**

    1.   This Identity Theft Prevention Program shall be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the District from identity theft.

    2.   The General Manager shall annually consider the District's experiences with identity theft situation, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the District maintains and changes in the District's business arrangements with other entities.

    3.   After considering these factors, the General Manager shall determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator shall update the Program or present the Board with his recommended changes and the shall make a determination of whether to accept, modify or reject those changes to the Program.

V.   **PROGRAM ADMINISTRATION**

A.   **Oversight**

Responsibility for implementing and updating this Program lies with the General Manager. The General Manager shall be responsible for the Program administration, for ensuring appropriate training of District staff, 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**

District staff responsible for implementing the Program shall be trained either by or under the direction of the General Manager in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.