APPENDIX C

STRASBURG SANITATION AND WATER DISTRICT
IDENTITY THEFT PREVENTION PROGRAM

This Identity Theft Prevention Program (this **"Program"**) has been adopted by the Strasburg Sanitation and Water District (the **"District"**) board of directors to comply with the Red Flags Rules located at 16 C.F.R. 681 and required by the Fair and Accurate Credit Transactions Act of 2003 which become effective November 1, 2009.

For the purposes of this Program, "**Identity Theft**" means any fraud committed or attempted using the personal identifying information of another person. "**Personal 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, but not limited to, any:

1. Name, social security number, date of birth, official government issued identification or number;
2. District account number;
3. Financial information such as bank account number or credit card number; or
4. Any unique electronic identification number, address or routing code.

Section 1 – "Red Flags"

The following shall be considered "Red Flags" relevant to the District.

1. Suspicious Documents

a. Identification documents that appear to be altered or forged;

b. Photographs or physical descriptions on documents that do not match the appearance of the person presenting the identification; or,

c. Information on identification documents is not consistent with readily accessible information that is on file, such as a signature card or a recent check.

2. Suspicious Personal Identifying Information

a. A Social Security Number (SSN) provided is the same as that of another person;

b. Failure or refusal to provide Personal Identifying Information upon request; or,

c. Personal Identifying Information is not consistent with other information on file.

3. Notice from Customers of Possible Identity Theft

Notification from a customer, victim, law enforcement authority, or any person that a fraudulent account has been opened for a person is engaged in identity theft.

Section 2 – Detecting Red Flags

District staff shall identify any Red Flags by examining documents carefully in the event any Personal Identifying Information is required in a transaction.

Section 3 – Response to Attempted/Suspected Fraudulent Use of Identity

Any District employee who detects a Red Flag must notify the District's administrator. If the administrator determines that the Red Flag evidences a risk of identity theft he or she will make reasonable efforts to notify the affected individual.

If identity theft has occurred, the Administrator may mitigate loss by:

1. Changing account numbers, passwords, security codes or security devices;
2. Close accounts; or
3. Take other actions deemed necessary.

Upon request, the administrator shall disclose to the affected individual the following information:

1. The type of identifying information involved;
2. The following telephone number that the person can call for further information and assistance;
    a. Local Law Enforcement,
    b. Federal Trade Commission: (Toll Free) 877-438-4338 or www.consumer.gov/idtheft
    c. Credit Reporting Agencies:
        i. Equifax: (800) 525-6285 or http://www.equifax.com
        ii. Experian: (800) 397-3742 or http://www.experian.com
        iii. TransUnion: (800) 916-8800 or http://www.transunion.com

Section 4 – Periodic Updates to the Program

The Administrator will update the Program periodically to reflect changes in risks to customers or to the safety and soundness of the District.

Section 5 – Employee Training

All employees with access to any customer Personal Identifying Information will be trained to identify and respond to Red Flags.