RESOLUTION 4-15-09
AMENDED
Lake Santee Regional Waste and Water District Resolution

Identity Theft Prevention Program

of

Lake Santee Regional Waste and Water District

13 SW Wrenn Parkway

Greensburg, IN 47240 – 7800

Resolution 4-15-2009 is amended to change the contact person and address.
The amendment was approved on 10-21-2010 and will replace the original in its entirety.

Be it hereby resolved by the Board of Trustees of the Lake Santee Regional Waste and Water District amends Resolution 4-15-09 passed on April 15, 2009 as follows:

Introduction:

The Lake Santee Regional Waste and Water District adopts an Identity Theft Prevention Program to identify "red flags" and assist customers and the public to help in the elimination and pr5evention of identity theft.

Program Purpose:

This program is intended to comply with the Federal Trade Commission's (FTC) Identity Theft "red flags" Rule. This plan is further intended to set forth an identity theft prevention program relevant to the operations of the Lake Santee Regional Waste and Water District.

Contact Information:

The Senior Management Person responsible for this plan is:
Name: Brandon Litmer
Title: Utility Superintendent
Phone Number: 812-527-9151

Risk Assessment:

The Lake Santee Regional Waste and Water District has conducted an internal risk assessment to evaluate how at risk the current procedures are for allowing customers to create a fraudulent account and evaluate if current (existing) accounts are being manipulated. This risk assessment evaluated how new accounts were opened and the methods used to access the account information. Using the assessment information the District was able to identify relevant "red flags" that were appropriate to prevent identity theft. Many "red flags" such as alerts from consumer reporting agencies are not relevant to the District. The District does not regularly obtain or store confidential customer social security numbers. In the event social security numbers or other highly sensitive information are gathered in the future, an additional assessment and an update program may be required.

Detection ("Red Flags"):

The Lake Santee Regional Waste and Water District adopts the following "red flags" to detect potentioan fraud. These are not intended to be all-inclusive and any and all suspicious activity, whether or not identified below as a "red flag:, may be investigated as necessary.

- Identification documents which appear to be altered
- Photo and physical description do not match appearance of applicant

- Other information is inconsistent with information provided by applicant
- Other information provided by applicant is inconsistent with information on file.
- Application appears to be altered or destroyed and reassembled
- Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application)
- Information commonly associated with fraudulent activity is provided by applicant (e.g. address that is a mail drop or prison, non-working phone number or associated with answering service/pager)
- Address or telephone # is the same as that of other customer at utility.
- Customer fails to provide all information requested.
- Personal information provided is inconsistent with information on file for a customer
- Identity theft is reported or discovered
- Fraud is reported by a consumer or customer report or reporting agency, credit freeze notices, or inconsistent activity patterns

---

"Red Flag" Reponse:

Any employee that may suspect fraud or detect a "red flag" will implement the following responses as applicable. All detections or suspicious "red flags" shall be reported to the Utility Superintendant.

- Ask applicant for additional documentation
- Notify the Utility Superintendant
- Notify law enforcement
- Decline to open the account
- Close the account
- Contact the consumer for verification or further information

---

Personal Information Security Procedures:

The following personal information security procedures must be utilized by all Lake Santee Regional Waste and Water District staff:

- Paper documents, files, and electronic media containing confidential personal information will be stored in locked file cabinets or locked room. Only specially identified employees will have access.
- Paper documents and files containing personally identifiable, confidential information are kept in locked file cabinets except when an employee is working on the file.
- Employees will not leave sensitive papers out on their desks when they are away from their workstations.

- Any sensitive information shipped will be shipped using a shipping service that allows tracking of the delivery of this information. Sensitive paper records will be shredded before being placed into the trash.
- Visitors who must enter area where sensitive files are kept must be escorted by an employee. No visitor will be given any entry codes or allowed unescorted access in the office.
- When installing new software, vendor-supplied default passwords will immediately be changed to a more secure strong password.
- Anti-virus and anti-spyware programs will be run on individual computers and on servers daily.
- When sensitive data is received or transmitted, secure connections will be used.
- Computer passwords will be required and will not be shared or posted near workstations.
- User names and passwords will be different and will not be shared or posted near workstations.
- The use of laptops is restricted to those employees who need them to perform their jobs.
- Laptop users will not store sensitive information on their laptops.
- If a laptop must be left in a vehicle, it is locked in a trunk or is otherwise covered such that it is not visible to a passerby looking through a window.
- The computer network will have a firewall where the network connects to the Internet.
- Any wireless network in use is secured.
- References will be checked or a background check will be performed before hiring employees who will have access to sensitive data.
- Procedures will be implemented to be certain that workers who leave employment no longer have access to sensitive information.
- Employees are required to notify the Utility Superintendant immediately if there is a potential security breach, such as a lost or stolen laptop.
- Electronic Fund Transfer registration forms require the names to be verified before the information is accepted for processing.

Identity Theft Prevention Program Review and Approval.

This plan has been reviewed and adopted by the Utility Board of Directors. Appropriate employees have been or will be trained on the contents and procedures of this Identity Theft Program.

Lake Santee Regional Waste and Water District Board of Directors:

Dated: October 21, 2010