SECTION 2 – APPENDIX 5

IDENTITY THEFT POLICY

I. History and Objective

This policy is developed pursuant to the Federal Trade Commission's Identity Theft Rules. *See* 16 C.F.R. § 681.2 *et seq*. The objective of this policy is to protect customers of Little Thompson Water District (hereinafter referred to as LTWD) from identity theft related to that customer's personal, family or household account.

II. POLICY

A. DEFINITIONS

1. Consumer Report is a communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living which will be used at least partly to determine the consumer's eligibility to receive and pay for water service.

2. Consumer Reporting Agency (CRA) is any agency/person which regularly engages in assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

3. Covered Account means a water utility account maintained by LTWD primarily for personal, family or household purposes.

4. Customer means a person that has a covered account with LTWD.

5. Identity Theft means a fraud committed or attempted using the identifying information of another person without authority.

6. Personal Identifying Information and Personal Information An individual's first name or initial and last name that may be used alone or in combination with any of the following: social security number, date of birth, driver license number, state identification number, passport number or other federal identification number, financial account numbers, and debit or credit card numbers.

7. Red Flags as used herein are patterns, practices or specific activities that indicate the possible occurrence of identity theft, including the following:

    a. Alerts, notifications, or other warnings received from CRAs which may include but are not limited to: fraud, a credit freeze, address discrepancy, or inconsistent pattern of account activity.

    b. The presentation of suspicious documents, such as: forged or altered

documents, inconsistencies between customer appearance and customer's photograph or physical description, or other inconsistent identification information provided by the customer.

c. The presentation of suspicious personal identifying information, such as: suspicious address change, failure by customer to provide required personal information, or the information provided by customer is not consistent with information on file.

d. The unusual use of, or other suspicious activity related to, a Covered Account such as: customer fails to make first payment, non-typical usage activity which is either extremely high or low, or bills sent to customer are returned as undeliverable although water is still being consumed at meter location.

e. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with Covered Accounts held by LTWD.

B. DUTIES TO PREVENT, DETECT AND MITIGATE

1. GENERAL
   a. All employees that have access to information in a Covered Account shall be trained to detect, and respond to, Red Flags.

   b. Means of customer identity verification may include:
      i. Full name;
      ii. Billing address;
      iii. Location/service address;
      iv. Phone number;
      v. For a U.S. person, one or more unexpired government-issued photo identification;
      vi. Social Security Number;
      vii. Passwords, security codes or other security devices (whether assigned by LTWD or user-defined);
      viii. Date of birth;
      ix. For a non-U.S. person, one or more of the following:
         1. Taxpayer identification number; passport number and country of issuance;
         2. Alien identification ("Green Card") card number;
         3. Number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

2. EMPLOYEE USE OF DATA
   Information requested about a customer's account by an individual, whether in person at the office or by telephone or other electronic means, is not to be divulged

until the identity of the person inquiring is confirmed to be the customer of record. Confirming information may include government issued identification forms such as a social security or driver's license number, date of birth, or any password given for identification on the account prior to proceeding with business. However, nothing in this policy shall prevent LTWD from transmitting information about the business and affairs of LTWD, including, but not limited to, its books and records, to any federal, state, or local law enforcement agency, administrative agency, or court as required or allowed by Colorado or federal law, rule or regulation.

3. ACCOUNT MANAGEMENT

a. New Accounts
   i. When opening new Covered Accounts and performing other functions regarding Covered Accounts including, but not limited to, address and billing changes, the identity of the applicant or customer shall be verified to the extent reasonable and practical under the circumstances.

   ii. LTWD should not open a new Covered Account if there is a fraud alert, active duty alert, or credit freeze for the applicant or customer unless LTWD gathers additional information sufficient to form a reasonable belief that the employee knows the identity of the applicant or customer making the request.

   iii. If one or more Red Flags are detected during the application process for a Covered Account or otherwise, the employee shall notify their supervisor, designated manager, or the privacy officer for LTWD.

b. Existing Accounts
   i. When servicing existing Covered Accounts, including, but not limited to, change of address requests, employees shall authenticate the identity of the customer as well as verify the change of address or other information on the account.

   ii. LTWD should not open a new Covered Account or make material changes to an existing Covered Account if there is a fraud alert, active duty alert, or credit freeze for the customer unless the employee gathers additional information sufficient to form a reasonable belief that the user knows the identity of the customer making the request.

   iii. If one or more Red Flags are detected while servicing a Covered Account, or otherwise, the employee shall notify their supervisor, designated manager, or the privacy officer for LTWD.

   iv. LTWD will flag or mark Covered Accounts that are to be monitored so that any employee servicing the account can be aware of the previous Red Flags to prevent and mitigate Identity Theft.

c. Closed Accounts

i. When closing a Covered Account or when accessing a closed Covered Account, LTWD shall ensure that any Personal Identifying Information is secure or remains secure and LTWD shall not disclose any Personal Identifying Information except as otherwise provided herein or as allowed by law or other LTWD policies, rules or regulations.

ii. If one or more Red Flags are detected when closing a Covered Account or when accessing a closed Covered Account, the employee shall notify their supervisor, designated manager, or the privacy officer for LTWD.

C. CONSUMER REPORTS

1. Use of Consumer Reports. Consumer Reports shall be used only in connection with the extension of credit, the extension of or provision of water service to a consumer, to review an account to determine if the consumer meets the terms of the account, collection of an account and for such other legitimate district purposes as may be allowed by law and approved by LTWD senior management.

D. PAPER FLOW AND ELECTRONIC ARCHIVING

1. Consumer Reports, Personal Identifying Information or other paper records containing Personal Information are not to be left on top of desks or files or other visible areas in offices or employee work areas outside of office hours. The foregoing items are to be put away out of sight or otherwise concealed when possible.

   a. Service orders and other documents dispatched to the field should not contain printed information on banking, social security, driver's license numbers, or other confidential information.

   b. Other personal information dispatched to the field should be limited to names, addresses and telephone numbers, non Personal Identifying Information where possible or other customer information necessary for water utility purposes.

2. After the records are archived, all original documents and paper copies thereof are to be disposed of securely or otherwise destroyed to prevent and mitigate Identity Theft.

E. COMPUTER ACCESS TO RECORDS

1. All persons or business affiliates (including all third party entities and vendors hired, retained or contracted with LTWD) with access to records containing Personal Identifying Information of customers shall be responsible for keeping their own computer information secure and inaccessible to others.

a. Employees are not to divulge personal log-in information for any of LTWD's systems or equipment to anyone unless otherwise provided herein or as otherwise may be allowed by law or other LTWD policies, rules or regulations.

b. Employees will ensure that district computers are password protected or otherwise secured at any time that employee is away from their computer as reasonably practical, and after work hours.

c. LTWD owned laptop computers or any other electronic device containing information about LTWD, its employees or customers are to be secured and protected while in the employee's possession. Such computers and electronic devices are not intended for non-company business or for use by anyone other than LTWD employees.

F. BREACH OF SECURITY

1. When any breach of security is discovered by an employee, or communicated to an employee by a customer, it should be reported immediately to the employee's direct supervisor, to their department manager or the privacy officer for LTWD.

   a. The Privacy Officer, or his/her designee shall immediately notify the affected customer(s) or employee(s) by telephone, if possible, followed with a written report of the circumstances and actions taken, both to reduce the possible damage caused by the security breach and to prevent similar breaches in the future.

2. Employee Breach of Security

   a. If an employee finds he/she has breached data security, he/she is to report it promptly to his/her direct supervisor. The direct supervisor will, in turn, report it to his/her department manager and/or the privacy officer for LTWD.

      i. The privacy officer is responsible for investigating the security breach.

      ii. If an employee is aware of but fails to report his/her own actions resulting in a breach of security, the employee may be subject to discipline, up to and including termination of employment.

   b. If an employee becomes aware of another employee's breach of security, he/she is to report it to his/her direct supervisor. The direct supervisor will report it to his/her department manager, who will report it to the privacy officer for LTWD. The privacy officer will inform the District Manager of any and all security breaches.

G. INTERNAL AND AWARENESS TRAINING

1. Training on the detection, prevention and mitigation of Identity Theft, privacy and security procedures, incident response and reporting procedures is necessary for all employees.

    a. Initial training on the foregoing items will be provided to all current and new employees by the privacy officer for LTWD.

    b. Additional training, including regular refresher classes, will be provided to all employees as necessary.

H. SERVICE PROVIDERS

1. If LTWD engages a service provider to perform an activity in connection with one or more Covered Accounts, LTWD shall take steps to ensure that such activity is conducted according to reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

2. Where appropriate, LTWD shall require by contract that service providers have policies and procedures to detect relevant Red Flags that may arise during performance of the services, and to either report the occurrence of the Red Flags to LTWD or to take appropriate steps to prevent or mitigate Identity Theft.

I. UPDATE AND COMPLIANCE REPORTS

1. This policy and the duties regarding the detection, prevention and mitigation of Identity Theft should be reviewed and updated periodically based upon the following:

    a. Experiences of LTWD with Identity Theft;

    b. Changes in methods of Identity Theft;

    c. Changes in methods to detect, prevent, and mitigate Identity Theft;

    d. Changes in the types of accounts that LTWD offers or maintains; and

    e. Changes in LTWD business arrangements which would impact this policy and the detection, prevention, and mitigation of Identity Theft, such as service provider arrangements.

2. The District Manager, privacy officer or his/her designee shall be responsible for implementation and administration of this policy. The privacy officer shall provide compliance reports at least annually to the Board of Directors, District Manager or other senior management official regarding LTWD’s compliance with applicable law.

3. The Board of Directors, District Manager, privacy officer or other senior management officials shall review the compliance reports and take appropriate action, if required.

4. Compliance reports should address material matters related to this policy and evaluate issues such as:

    a. The effectiveness of LTWD's policies and procedures;

    b. Service provider arrangements;

    c. Significant incidents involving Identity Theft and management's response; and

    d. Recommendations for material changes to this policy and the detection, prevention and mitigation of Identity Theft.

III. RESPONSIBILITIES

A. BOARD OF DIRECTORS

The Board of Directors is responsible for approval of this policy as well as changes and revisions to this policy.

B. DISTRICT MANAGER

The District Manager will keep the Board of Directors informed and provide them with annual reports.

C. PRIVACY OFFICER

The privacy officer shall oversee the overall application of this policy.

D. EMPLOYEES

All employees are responsible for protecting Personal Identifying Information in any form that is collected and maintained by LTWD; for detecting, preventing and mitigating identity theft; and for promptly reporting any breach of security that becomes known to them.