**May 22, 2024**

Kempner Water Supply Corporation

# Red Flags
# Identity Theft
# Prevention Program
# Compliance

All utilities are required to comply with this regulation. The Red Flag Rule requires any entity where there is a risk of identity theft, to develop and implement an Identity Theft Prevention Program. The Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft. The rule was issued by the Federal Reserve System, the Federal Deposit Insurance Corporation, the Federal Trade Commission, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision. The compliance date is November 1, 2008, and includes all U.S. utilities.

**All utilities are required to comply with the Federal Trade Commission's "Red Flags Rule for Identity Theft" even if only nominal information such as name, phone number and address are collected.**

The primary purpose of the rule is to protect against the establishment of false accounts and ensure existing accounts are not being manipulated. This regulation does not address or require utilities to adopt measures that will protect consumer information and prevent unauthorized access. However, implementation of good management practices to protect personal consumer data can prevent identity theft.

Steps required for annual review of the individual Identity Theft Prevention Program:

- □ Assess existing identity theft risk for new and existing accounts.
- □ Use the risk assessment to select measures (red flags) that may be used to detect attempts to establish fraudulent accounts.
- □ Identify procedures for employees to prevent the establishment of false accounts and procedures for employees to implement if existing accounts are being manipulated.
- □ Train the appropriate employees on the program's policies and procedures.
- □ Update the plan annually with review and approval by the governing body or designated senior management. The annual report should address any material matters related to the program such as the effectiveness of the policies and procedures, the oversight and effectiveness of any third-party billing and account establishment entities, a summary of any identity thefts incidents and the response to the incident, and recommendations for substantial changes to the program, if any.

# Identity Theft Prevention Program
# For
# Kempner Water Supply Corporation
# PO Box 103
# Kempner, TX 76539
# May 24, 2023

This Program is intended to identify red flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, methods to ensure existing accounts were not opened using false information, and measures to respond to such events.

**Contact Information:**

The Senior Management Person responsible for this program is:
Name: Bruce Sorenson
Title: General Manager
Phone number: 512-932-3701

The Governing Board Members of the Kempner Water Supply Corporation are:

Dennis Kliza, President

Sam Kier, Vice President

Ric Dominowski, Secretary/Treasurer

Kara Bathurst, Director

Stella Clements, Director

Paul Williams, Director

John Daugherty, Director

Billy Malady, Director

Dan Christy, Director

## Risk Assessment

The Kempner Water Supply Corporation (KWSC) has conducted an internal risk assessment to evaluate how at risk the current procedures are at 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 this information, the utility was able to identify red flags that were appropriate to prevent identity theft:

- New accounts opened In Person
- New accounts opened via Telephone
- New accounts opened via Fax
- New accounts opened via Web
- Account information accessed In Person
- Account information accessed via Telephone (Person)
- Account information is accessed via Web Site
- Identity theft occurred in the past from someone falsely opening a utility account

---

**Detection (Red Flags):**

The KWSC adopts the following red flags to detect potential fraud. These are not intended to be all-inclusive, and other suspicious activity may be investigated as necessary:

- Inconsistent activity patterns indicated by consumer report such as:
    - Recent and significant increase in volume of inquiries
    - Accounts closed for cause or abuse
- Identification documents appear to be altered
- Photo and physical description do not match appearance of applicant
- Other information is inconsistent with information provided by applicant
- Personal information provided is inconsistent with information on file for a customer
- Application appears altered or destroyed and reassembled
- Personal information provided by applicant does not match other sources of information (SS# not issued or listed as deceased)
- Lack of correlation between the SS# range and date of birth
- Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application)
- SS#, address, or telephone# is the same as that of another customer at utility
- Customer fails to provide all information requested
- Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet
- Identity theft is reported or discovered

---

**Response**

Any employee that may suspect fraud or detect a red flag will implement the following response as applicable. All detections or suspicious red flags shall be reported to the general manager.

- □ Ask applicant for additional documentation.
- □ Any employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customer's identity must notify the General Manager.
- □ Do not open the account.
- □ Close the account.
- □ Do not attempt to collect against the account but notify authorities

---

**Administrative Security - All Areas of PII – Personal Identifiable Information:**

The KWSC adopts the following security procedures to protect consumer information and to prevent unauthorized access:

- □ Paper documents, files, and electronic media containing secure information are stored in locked file cabinets.
- □ Only specially identified employees with a legitimate need will have keys to the cabinet.
- □ Files containing personally identifiable 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.
- □ Employees store files when leaving their work areas
- □ Employees log off their computers when leaving their work areas
- □ Employees lock file cabinets when leaving their work areas
- □ Access to offsite storage facilities is limited to employees with a legitimate business need.
- □ Any sensitive information shipped will be shipped using a shipping service that allows tracking of the delivery of this information.
- □ Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the utility.
- □ No visitor will be given any entry codes or allowed unescorted access to the office.
- □ Access to sensitive information and computers will be controlled using "strong" passwords. Employees will choose passwords with a mix of letters, numbers, and characters.
- □ Usernames and passwords will be different.
- □ Passwords will not be shared or posted near workstations.
- □ Password-activated screen savers will be used to lock employee computers after a period of inactivity.
- □ The computer network will have a firewall where network connects to the internet.
- □ 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.
- □ Any wireless network in use is secured.
- □ The use of laptops is restricted to those employees who need them to perform their jobs.
- □ Laptops are stored in a secure place.

□ Laptop users will not store sensitive information on their laptops.
□ Employees never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage.
□ If a laptop must be left in a vehicle, it is locked in a hidden place.
□ Employees are required to notify the general manager immediately if there is a potential security breach, such as a lost or stolen laptop.
□ Check references or do background checks before hiring employees who will have access to sensitive data.
□ New employees sign an agreement to follow your company's confidentiality and security standards for handling sensitive data.
□ Access to customer's personal identity information is limited to employees with a "need to know."
□ Procedures exist for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information.
□ Implement a regular schedule of employee training.
□ Employees will be alerted to attempts at phone phishing.
□ Employees who violate security policy are subjected to discipline, up to, and including, dismissal.
□ Service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of our data.
□ Paper records will be shredded before being placed into the trash.
□ Paper shredders will be available at each desk in the office, next to the photocopier, and at the home of any employee doing work at home.
□ Any data storage media will be disposed of by shredding, punching holes in, or incineration.

---

A report will be prepared annually and submitted to the senior management or governing body to include matter related to the program, the effectiveness of the policies and procedures, the oversight and effectiveness of any third-party billing and account establishment entities, a summary of any identity theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.

2023-2024: No incidents have been identified or reported since the last program review.

## Identity Theft Prevention Program Review and Approval

This plan has been reviewed and adopted by the KWSC Board of Directors on May 22, 2024. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Program.

Kempner Water Supply Corporation
RED FLAG’S IDENTITY THEFT PREVENTION PROGRAM
May 22, 2024

The Board of Directors of Kempner Water Supply Corporation ("KWSC") approved this Identity Theft Prevention Program ("Program") at a held meeting on **May 22, 2024**. The Program was developed to comply with the Federal Trade Commission's Identity Theft Prevention Red Flags Rule (16 CFR § 681.2). This Program has been created in consultation with administrative staff and clerks, after assessing risk of Identity Theft associated with Member and Customer Accounts.

## I. **Definitions**

For purposes of the Program, the following terms are defined as:

> **"Member Account"** means (i) any person, partnership, cooperative corporation, corporation, agency, or public or private organization that has qualified for service and received a Membership in accordance with the Corporation's Tariff, and (ii) any other account KWSC identifies as having a reasonably foreseeable risk to customers or to the safety and soundness of KWSC from Identity Theft. The following (3) three types of accounts are Covered Accounts.
>
> 1) Active membership account
> 2) Inactive membership account
> 3) Rental accounts

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

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

## II. Program Purposes

The purposes of the Program are to:

1) Identify the relevant Red Flags based on the risk factors associated with KWSC's covered accounts.
2) Corporation policies and procedures for detecting Red Flags.
3) Identify steps the Corporation will take to prevent and mitigate Identity Theft; and
4) Create a system for regular updates and administrative oversight to the Program.

## III. **Identification of Red Flags**

The Identity Theft Red Flags Mitigation and Resolution Procedures (Appendix A) identifies the Red Flags that would be most relevant to KWSC. The Red Flags generally fall within one of the following [five] general types of Red Flags:

1) Requested Documentation not provided upon multiple requests.
2) Suspicious Documents.
3) Suspicious Personal Identifying Information.

4) Suspicious or Unusual Use of Covered Account; and
5) Alerts from others (e.g., customer, Identity Theft victim, or law enforcement)

## IV. **Detection of Red Flags**

In order to facilitate detection of the Red Flags identified in Appendix A, KWSC staff will take the following steps to obtain and verify the identity of the person.

A. **New Accounts**

1) Require identifying information (e.g., full name, date of birth, address, government issued ID, insurance card, etc.)
2) Proof of Ownership,
3) Copy of Survey and/or Plat
4) Recorded Power of Attorney, if applying for the owner on their behalf

B. **Existing Accounts**

1) Verify validity of requests for changes of billing address accepted in writing only
2) Verify identification of customers before giving out any personal information
3) Verify appropriate legal documentation prior to membership transfer to a surviving spouse, children, heirs, executors and/or trustee's

C. **Bank Draft**

1) Verify validity of request to participate with the Bank Draft Program
2) Verify identification of customer and signature prior to them requesting banking information to be changed.
3) Follow all ACH and NCH banking guidelines
4) Bank Draft forms will be kept in a locked filing cabinet

## V. **Preventing and Mitigating Identity Theft**

In order to prevent and mitigate the effects of Identity Theft, staff will follow the appropriate steps identified in the attached Identity Theft Red Flags Mitigation and Resolution Procedures (Appendix A).

## VI. **Program Administration**

The Executive Committee is responsible for developing, implementing, administering, and updating the Program. **General Manager** will be responsible for developing a training program for staff identified by **Office Manager** as responsible for or having a role in implementing the Program.

## VII. **Updating of Program**

The **Policy Committee** will annually review the Program and update the Program to reflect changes in risks to customer/member covered account holders from Identity Theft.

## Attachment A
## Relevant Identity Theft Red Flags Mitigation and Resolution Procedures

| IDENTITY THEFT RED FLAG | PREVENTION/MITIGATION PROCEDURE | RESOLUTION OF RED FLAG |
|---|---|---|
| Documents provided for identification appear to have been altered or forged. | Stop the application/billing process and require applicant to provide additional satisfactory information to verify identity. | Additional documentation must be provided to resolve discrepancy and continue application/billing process. |
| Personal identifying information provided by the member/customer is not consistent with other personal identifying information provided by the member/customer. | Stop the application/billing process and require applicant to provide additional satisfactory information to verify identity. | Additional documentation must be provided to resolve discrepancy and continue application/billing process. |
| KWSC is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft. | Investigation to determine if billing was made fraudulently. | Additional documentation must be provided to resolve discrepancy and continue admissions/billing process. Contact insurance company as necessary.<br>Notify law enforcement as appropriate.<br>If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with customer/member. |
| Mail sent to the customer/member is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the member/customers covered account. | Appropriate procedures are used to find the customer/members current mailing address. | Member/Customer is found, and contact information is updated. |