Wisconsin Rural Water Association

Identity Theft Prevention Program Compliance Model

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 May 1, 2009 and includes all U.S. utilities.

Wisconsin Rural Water Association
Identity Theft Prevention Program Compliance Model

This model has been designed to assist water and wastewater utilities in complying with the Federal Trade Commission's (FTC) Identity Theft Red Flag Rule. The rule requires utilities to develop an "Identity Theft Prevention Program." The program consists of selecting methods to detect red flags when accounts are fraudulent, procedures to prevent the establishment of false accounts, procedures to ensure existing accounts are not being manipulated, and procedures to respond to identity theft.

All utilities are required to comply with the FTC's "Identity Theft Red Flag Rule" even if only nominal information such as name, phone number and address are collected. However, the true risk established through the risk assessment activity may not require any changes to existing policies or procedures.

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. Appendix A is a list of other security procedures a utility should consider to protect consumer information and to prevent unauthorized access.

Steps required to develop a utility's individual Identity Theft Prevention Program:

- Assess their existing identity theft risk (risk assessment) 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.
- Obtain program approval by the governing body or designated senior management by May 1, 2009.
- 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
Utility Name
Address
City, State, Zip
Date

Utility Name Identity Theft Prevention Program

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: _____

Title: _____

Phone number: _____

The Governing Body Members of the Utility are:

Board Members:

1._____

2._____

3._____

4. _____

5._____

6._____

Risk Assessment

The *Utility Name* 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. *Add or delete items as applicable:*

- ❑ 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 Telephone (Automated)
- ❑ Account information is accessed via Web Site
- ❑ Identity theft occurred in the past from someone falsely opening a utility account

---

Detection (Red Flags):

The *Utility Name* 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. *Add or delete items as applicable:*

- ❑ Fraud or active duty alerts included with consumer reports
- ❑ Notice of credit freeze provided by consumer reporting agency
- ❑ Notice of address discrepancy provided by consumer reporting agency
- ❑ Inconsistent activity patterns indicated by consumer report such as:
    - o Recent and significant increase in volume of inquiries
    - o Unusual number of recent credit applications
    - o A material change in use of credit
    - o 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
- ❑ Other information provided by applicant is inconsistent with information on file.
- ❑ Application appears altered or destroyed and reassembled
- ❑ Personal information provided by applicant does not match other sources of information (e.g. credit reports, 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)

- ❑ 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)
- ❑ SS#, 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
- ❑ 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 senior management official. *Add or delete items as applicable:*

- ❑ Ask applicant for additional documentation
- ❑ Notify internal manager: Any utility employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers identity must notify _____
- ❑ Notify law enforcement: The utility will notify _____ at _____ of any attempted or actual identity theft.
- ❑ Do not open the account
- ❑ Close the account
- ❑ Do not attempt to collect against the account but notify authorities

---

Personal Information Security Procedures:

The *Utility Name* adopts the following security procedures: *(select appropriate procedures from Appendix A and add other procedures as appropriate).*

1.
2.
3.
4.

Identity Theft Prevention Program Review and Approval

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

Signatures:

1._____ Date_____

2._____ Date_____

3._____ Date_____

4._____ Date_____

5._____ Date_____

6._____ Date_____

If no Board of Directors, this plan has been reviewed and adopted by:

Name of Senior Management Staff Person: _____

Position: _____

Date: _____

Signature: _____

A report will be prepared annually and submitted to the above named 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 identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.