



**NATIONAL RURAL WATER
ASSOCIATION**

**National Rural Water Association
Identity Theft Prevention Program Guidance**

September 25, 2008

National Rural Water Association

Identity Theft Prevention Program Guidance

Executive Summary:

The Federal Trade Commission has issued a regulation, the “Identity Theft Red Flags Rule”. The rule requires covered institutions to develop an Identity Theft Prevention Program. The following is a brief summary of the rules requirements

- 1. What is the intent of the rule? - The purpose of the rule is to detect, prevent, and mitigate against identity theft**
- 2. Who is required to comply? - Utilities that bill customers after they have provided water/wastewater service, financial institutions, and creditors must comply with the regulation**
- 3. What do I have to do? - A written Identity Theft Prevention Program must be developed that contains the procedures to detect, prevent and respond to attempts at opening up false accounts. And a program to determine if existing accounts have abnormal activity or are being manipulated (i.e. illegal use of water). The program must be updated and a report generated annually that is approved by the Utility Board of Directors or senior management (if a board does not exist).**
- 4. When is the deadline for compliance? - The Identity Theft Prevention Program must be developed, approved, and appropriate employees trained by November 1, 2008**

Overview

This model has been designed to help water and wastewater utilities comply with the Federal Trade Commission's (FTC) "Identity Theft Red Flags Rule". The rule requires utilities, financial institutions and creditors to develop an Identity Theft Prevention Program. The primary purpose of the rule is to protect against the establishment of false accounts and ensure existing accounts are not being manipulated or have an abnormal use of water.

Utilities are first required to assess their existing identity theft risk for new and existing accounts. Using this information measures are selected that would be used to detect attempts to establish fraudulent accounts (red flags). The final step is identifying procedures for employees to prevent the establishment of false accounts and procedures to monitor if existing accounts are being manipulated.

Appendix A is a list of other security procedures a utility should consider to protect consumer information and to prevent unauthorized access. This regulation does not require utilities to adopt these measures; however, implementation of appropriate measures is a good management practice to protect personal consumer data.

All utilities are required to comply with the FTC's "Identity Theft Red Flags Rule" unless they bill for water/wastewater service before providing the service. Utilities that only collect nominal information such as name, phone number and address are still required to comply. However, the actual identity theft risk established thru the risk assessment activity may justify no changes to existing policies or only require minor changes to incorporate relevant detection methods (red flags).

The information collected through this process should be used to develop the utility's "Identity Theft Prevention Program". The Program should incorporate the policies and procedures including the red flags and the necessary actions employees should implement if a false account is attempted to be opened and the measures to take if an existing account is manipulated. All utilities are required to have their Program developed, approved by the board or designated employee at the level of senior management (DESM), and the appropriate employees trained by November 1, 2008. This guide can be used to collect the information for a written utility specific program.

Lastly, the plan must be updated periodically. An annual report must be reviewed and approved by the utilities board or DESM. The 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).