

# **DRAFT National Rural Water Association Identity Theft Program Model**

**September 22, 2008**

**This model has been designed to help water and wastewater utilities comply with the Federal Trade Commission's (FTC) "Identity Theft Red Flags Rule". National Rural Water Association developed the model and the FTC has reviewed, provided input which was incorporated, and confirmed that the model is consistent with their regulation. The rule requires utilities to develop a Identity Theft Program. The primary purpose of the rule is to protect against the establishment of false accounts and ensure existing accounts were not opened using false information. 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 for employees to implement if it is discovered that an existing account was opened using false information. 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". Utilities that only collect nominal information such as name, phone number and address, or utilities that rely on the local assessment and taxation office to direct them to open accounts 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 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 discovered that had been created using false identification. 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.**

**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).**

## **(1) System Info**

Address

City, State, Zip

Phone

Fax

Email

Number of Accounts/Connections/Taps:

Annual Revenue:

## **(2) Contact Info**

1. Who is the designated employee at the level of senior management who is responsible for the Identity Theft Program (Name, Title, Phone, Email)

## **(3) Board Members**

1. \_\_\_\_\_

2. \_\_\_\_\_

3. \_\_\_\_\_

4. \_\_\_\_\_

5. \_\_\_\_\_

6. \_\_\_\_\_

## **(4) Risk Assessment**

Each utility must complete an internal risk assessment to evaluate how at risk the current procedures are at allowing customers to create a false account and evaluate if current (existing) accounts could have been opened using false information. The primary means to assess your current risks is summarized in Section 4.1. These include methods a utility uses to open accounts, methods to access

account information, and any information on actual identity thefts that may have occurred in the past. Information collected from section 4.2 can be used to help inform a utilities decision about their existing risk .

## **(4.1) Primary Risk Assessment**

1. Are new accounts opened In Person
2. Are new accounts opened via Telephone
3. Are new accounts opened via Fax
4. Are new accounts opened via Web
5. Is account information accessed In Person
6. Is account information accessed via Telephone (Person)
7. Is account information accessed via Telephone (Automated)
8. Is account information accessed via Web Site
9. Has identity theft occurred in the past from someone falsely opening up a utility account? If so, have you adopted procedures to protect against the occurrence(s)?

## **(4.2) Other Risk Factors**

10. Do you collect sensitive credit data from applicants? Yes/No  
(This data includes 1 or more of the following items.)
  - a. Name
  - b. SSN
  - c. Birth Date
  - d. Drivers license number
  - e. Alien registration number
  - f. Passport number
  - g. Employee identification number
  - h. Payment history from previous utilities
  - i. Bank/checking/savings Routing numbers

- j. Bank/checking/savings Account numbers
  - k. Credit Card Account Numbers
11. Do you request consumer credit reports from Experian, Tran Union, Equifax or others?
  12. Do you file address discrepancies or file late payments to consumer reporting agencies?
  13. Do you accept credit cards or debit cards for payment?
  14. Do you validate applicant's SSN?
  15. Do you currently have existing policies and procedures to protect against identity theft?

## **(5) Detection (Red Flags):**

How do you detect potential fraud?

1. Fraud or active duty alerts included with consumer reports
2. Notice of credit freeze provided by consumer reporting agency
3. Notice of address discrepancy provided by consumer reporting agency
4. Inconsistent activity patterns indicated by consumer report such as:
  - a. Recent and significant increase in volume of inquiries
  - b. Unusual number of recent credit applications
  - c. A material change in use of credit
  - d. Accounts closed for cause or abuse
5. Identification documents appear to be altered
6. Photo and physical description do not match appearance of applicant
7. Other information is inconsistent with information provided by applicant
8. Other information provided by applicant is inconsistent with information on file.
9. Application appears altered or destroyed and reassembled
10. Personal information provided by applicant does not match other sources of information (e.g. credit reports, SS# not issued or listed as deceased)
11. Lack of correlation between the SS# range and date of birth
12. Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application)
13. 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)
14. SS#, address, or telephone # is the same as that of other customer at utility
15. Customer fails to provide all information requested
16. Personal information provided is inconsistent with information on file for a customer

17. Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet
18. Identity theft is reported or discovered

## **(6) Response**

How do you respond to suspected fraud?

1. Ask applicant for additional documentation
2. 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 \_\_\_\_\_
3. Notify law enforcement: The utility will notify \_\_\_\_\_ at \_\_\_\_\_ of any attempted or actual identity theft.
4. Place fraud Alerts with Credit Reporting Agencies
5. Do not open the account
6. Close the account

## **Appendix A**

### **Other Security Procedures**

1. Paper documents, files, and electronic media containing secure information will be stored in locked file cabinets. File cabinets will be stored in a locked room.
2. Only specially identified employees with a legitimate need will have keys to the room and cabinet.
3. Files containing personally identifiable information are kept in locked file cabinets except when an employee is working on the file.
4. Employees will not to leave sensitive papers out on their desks when they are away from their workstations.
5. Employees store files when leaving their work areas
6. Employees log off their computers when leaving their work areas
7. Employees lock file cabinets when leaving their work areas
8. Employees lock file room doors when leaving their work areas
9. Access to offsite storage facilities is limited to employees with a legitimate business need.
10. Any sensitive information shipped using outside carriers or contractors will be encrypted
11. Any sensitive information shipped will be shipped using a shipping service that allows tracking of the delivery this information.
12. Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the utility.
13. No visitor will be given any entry codes or allowed unescorted access the office.
14. Access to sensitive information will be controlled using “strong” passwords. Employees will choose passwords with a mix of letters, numbers, and characters. User names and passwords will be different. Passwords will be changed at least monthly.
15. Passwords will not be shared or posted near workstations.
16. Password-activated screen savers will be used to lock employee computers after a period of inactivity.

17. When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
18. Sensitive consumer data will not be stored on any computer with an Internet connection
19. Sensitive information that is sent to third parties over public networks will be encrypted
20. Sensitive information that is stored on computer network or portable storage devices used by your employees will be encrypted.
21. Email transmissions within your business will be encrypted if they contain personally identifying information.
22. Anti-virus and anti-spyware programs will be run on individual computers and on servers daily.
23. When sensitive data is received or transmitted, secure connections will be used
24. Computer passwords will be required.
25. Employees will use passwords with a mix of letters, numbers, and characters.
26. User names and passwords will be different.
27. Passwords will be changed at least monthly.
28. Passwords will not be shared or posted near workstations.
29. Password-activated screen savers will be used to lock employee computers after a period of inactivity.
30. When installing new software, vendor-supplied default passwords are changed.
31. The use of laptops is restricted to those employees who need them to perform their jobs.
32. Laptops are stored in secure place.
33. Laptop users will not store sensitive information on their laptops.
34. Laptops which contain sensitive data will be encrypted
35. Employees never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage.
36. If a laptop must be left in a vehicle, it is locked in a trunk.
37. The computer network will have a firewall where your network connects to the Internet.

38. Any wireless network in use is secured.
39. Maintain central log files of security-related information to monitor activity on your network.
40. Monitor incoming traffic for signs of a data breach.
41. Monitor outgoing traffic for signs of a data breach.
42. Implement a breach response plan.
43. Check references or do background checks before hiring employees who will have access to sensitive data.
44. New employees sign an agreement to follow your company's confidentiality and security standards for handling sensitive data.
45. Access to customer's personal identify information is limited to employees with a "need to know."
46. 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.
47. Implement a regular schedule of employee training.
48. Employees will be alert to attempts at phone phishing.
49. Employees are required to notify the general manager immediately if there is a potential security breach, such as a lost or stolen laptop.
50. Employees who violate security policy are subjected to discipline, up to, and including, dismissal.
51. 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.
52. Paper records will be shredded before being placed into the trash.
53. 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.
54. Any data storage media will be disposed of by shredding, punching holes in, or incineration.