



**American Water Works
Association**

The Authoritative Resource on Safe Water™

Government Affairs Office
1300 Eye Street NW
Suite 701W
Washington, DC 20005 3314
T 202.628.8303
F 202.628.2816

Headquarters Office
8666 West Quincy Avenue
Denver, CO 80235-3098
T 303.794.7711
F 303.347.0804
www.awwa.org

AWWA Red Flag Template



Introduction

On November 9, 2007, the Federal Trade Commission (FTC) and several other Federal agencies published the Identity Theft Red Flag Rule (FR 72:217:63717). All utilities that provide water/wastewater service on credit, i.e., send a bill for past service, are required to develop a program to comply with this rule by November 1, 2008.

The Identity Theft Red Flag Rule requires any creditor to develop a program to detect, prevent, and mitigate identity theft. Utility companies are specifically mentioned in the definition of a creditor, so this Rule clearly applies to water and wastewater utilities.

A Red Flag is “a pattern, practice, or specific activity that indicates the possible existence of identity theft”. Identity Theft is “a fraud committed or attempted using the identifying information of another person without authority”.

This template should be used as a starting point for compliance with this Rule. Utilities may need to adjust this template according to match existing business practices, and additional Red Flags may be found beyond the ones listed in the Red Flag Guidelines in the *Federal Register* notice (Page 63774). The utility program does not necessarily have to be extremely complex, and many existing utility business practices will help in complying with this rule. Nothing has to be sent in to Federal Trade Commission (FTC) or any other federal agency, but the program information and documentation needs to be kept on file.

For more information, this rule can be found online at <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>

At first glance, the *Federal Register* notice is rather lengthy (over 60 pages), but most of this Rule is directed towards banks and financial institutions as this is a multi-agency Rule. The only relevant regulatory language for utilities is the FTC portion of the Rule on last six pages (pages 63771-63775) of the *Federal Register* notice. The FTC Rule is three pages and the last three pages are the interagency guidance that gives more details on what to consider when designing your program.

IDENTITY THEFT PREVENTION PROGRAM

Developed By and For:

(Utility Name)

Approval of the Initial Program Received From:

(Utility's Governing Body)

On the Following Date:

Program Reviewed, Updated and Approved on:

Table of Contents

Part I.	Assessment of Existing Business Practices.....	Page 1
Part II.	Identification of Red Flags.....	Page 2
Part III.	Detection of Red Flags.....	Page 3
Part IV.	Prevention and Mitigation.....	Page 4
Part V.	Program Administration.....	Page 5
	A. Staff Training	Page 5
	B. Program Review and Update.....	Page 5
	C. Program Approval and Adoption.....	Page 5
	D. Annual Reporting.....	Page 6
	E. Service Provider Oversight.....	Page 6
Part VI.	Additional Security Information.....	Page 7

Part I. Assessment of Existing Business Practices

Part I of the Identity Theft Prevention Program is used to identify areas of potential risk within the Utility’s standard Customer Service business practices. The Utility has selected specific business processes associated with offering or maintaining accounts, or engaging in other activities, that could raise “red flags” indicating the potential for identity theft. It should be noted that the business practices listed below are typical for most utilities that operate as retailers or wholesalers of drinking water.

- A. Utility provides Customer Service personnel with the ability to request and review a customer’s personal identifying information when engaging in any of the following activities:
- Open new accounts;
 - Access existing accounts;
 - Modify existing accounts; and/or
 - Close existing accounts.
- B. Utility provides customers with the ability to do one or more of the following actions independent of Customer Service personnel (either through an automated phone system or online), and a customer’s personal identifying information is required to complete any of these activities:
- Open a new account;
 - Access an existing account;
 - Modify an existing account; and/or
 - Close an existing account.

Also, if the Utility has identified a past occurrence of identity theft that was linked to a customer’s utility account (an unauthorized opening, modifying or closing of an account), then they must perform the actions set forth in the following Program.

Part II. Identification of Red Flags

Part II of the Identity Theft Prevention Program assists the Utility in identifying Red Flags that may arise during routine handling of new and/or existing accounts. The Utility has identified the following items as potential Red Flag sources or categories that might indicate an instance of identity theft.

- Consumer report includes a fraud or active duty alert, a notice of credit freeze and/or a notice of address discrepancy.
- Documents provided for identification appear to have been altered or forged.
- Photograph, physical description and/or other information on the identification is not consistent with the appearance of the person presenting the identification.
- Information on the identification is not consistent with readily accessible information that is on file with the Utility, such as property tax records.
- Information provided is inconsistent when compared against external information sources (address does not match any address in the consumer report and/or social security number has not been issued or is associated with a deceased person).
- Information provided by the customer is inconsistent with other information provided by the customer (no correlation between SSN range and date of birth).
- Information provided is associated with known fraudulent activity (address and/or phone number on an application is the same as the address provided on a previous fraudulent application).
- Information provided is of a type commonly associated with fraudulent activity (address on an application is fictitious and/or phone number is invalid).
- Social security number, address and/or telephone number provided is the same as or similar to ones provided by another customer.
- Customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- Customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account
- Utility is notified that the customer is not receiving paper account statements.
- Utility is notified that it has opened a fraudulent account for a person engaged in identity theft.

Part III. Detection of Red Flags

Part III of the Identity Theft Prevention Program addresses the process of detecting Red Flags as related to possible identity theft during the Utility's routine handling of new and/or existing accounts. The following is a list of detection methods that the Utility uses to prevent identity theft.

- Require customers to present government-issued identification information to open a new account. Types of necessary information include:
 - Name
 - Date of birth
 - Social security number
 - Address
 - Phone number
 - Photo identification
- Verify personal identification information using records on file with the Utility or through a third-party source such as a consumer reporting agency.
- Independently contact the customer (in the case of phone or internet setup of new utility accounts).
- When fielding a request to access and/or modify an existing account (such as a change of billing address), verify identity of customer by requesting specific pieces of personal identifying information (identification with the new billing address and/or documentation proving shift of financial liability)
- If new banking information is provided for electronic payment of accounts, cross-check ownership of the new banking account with the customer name on the utility account by contacting the appropriate financial institution.
- For online or automated phone system access of utility account, require the establishment of security questions during the initial set-up of the account.

Part IV. Prevention and Mitigation

Part IV of the Identity Theft Prevention Program details response actions for Utility personnel if the personnel have observed a Red Flag associated with a new or existing utility account. One or more of the following actions will be taken by the Utility to rectify the situation.

- Utility will not open a new account (after review of the presented identifying information and discussion with department supervisor)
- For an existing account, the Utility may discontinue the services associated with that account and/or:
 - Continue to monitor the account for evidence of identity theft and contact the customer to discuss possible actions.
 - Change the passwords, security codes, or other security devices that permit access to an existing account.
 - Reopen an existing account with a new account number.
 - Close an existing account.
- If the Utility has identified an instance of identity theft associated with an unpaid account, the Utility will not attempt to collect on the account or sell the account to a debt collector.
- If applicable, the Utility will provide the consumer reporting agencies with a description of the identity theft event.
- For all instances of suspected or confirmed identity theft, the Utility will notify local law enforcement and will provide them with all the relevant details associated with the identity theft event.

Part V. Program Administration

Program administration is an important part of the Identity Theft Prevention Program. This section details the training requirements, annual program review, approval and adoption process and annual reporting requirements that are associated with this Program.

A. Staff Training

Any employee with the ability to open a new account, or access/manage/close an existing account will receive training on identifying and detecting Red Flags. They will also be trained in the appropriate response actions in the event that an instance of identity theft is suspected. Key management personnel in appropriate departments will also receive training on the contents of this Program. As necessary, employees will be re-trained annually if the Program is updated to include new methods of identifying and detecting Red Flags, or if new response actions are implemented.

B. Program Review and Update

The Utility will review and update the Program annually to reflect changes in risks to customers from identity theft based on factors such as:

- Experiences of the Utility with identity theft.
- Changes in methods of identity theft.
- Changes in methods to detect, prevent, and mitigate identity theft.
- Changes in the types of accounts that the Utility offers or maintains.
- Changes in the business arrangements of the Utility, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

C. Program Approval and Adoption

This Program has been reviewed and approved by the Utility's appropriate governing body (examples include the Board of Directors, a City/Town/County Council, or the Commissioners).

The Utility's governing body has assigned the following Utility staff member, _____, to be responsible for the oversight, development, implementation and administration of the Program. Annually, the designated staff member will develop the annual report as described in Section D that will address compliance of the Utility with this Program. The Utility's governing body is responsible for reviewing this reports and approving material changes to the Program as necessary to address changing identity theft risks.

D. Annual Reporting

The Utility will provide an annual report to the appropriate governing body of the Utility that details the Utility's compliance with the Federal Trade Commission's Red Flags Rule. The report will address matters related to the Program and address several topic areas including:

- Effectiveness of the policies and procedures of the Utility in addressing the risk of identity theft in connection with the opening of new accounts and with respect to the management of existing accounts;
- Service provider arrangements;
- Significant incidents involving identity theft and management's response; and,
- Recommendations for material changes to the Program.

E. Service Provider Oversight

Whenever the Utility engages a service provider to perform an activity in connection with one or more of the customer accounts, the Utility will verify that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. To accomplish this, the Utility will require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the Utility, or to take appropriate steps to prevent or mitigate identity theft.

Part VI. Additional Security Information

While utilities are not required by the Federal Trade Commission to implement the following business practices, they are provided as suggestions to assist utilities in the prevention of identity theft. Utilities should consider:

1. Checking references or doing background checks before hiring employees who will have access to customer information.
2. Asking every new employee to sign an agreement to follow the Utility's confidentiality and security standards for handling customer information.
3. Limiting access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.
4. Controlling access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis. Using password-activated screen savers to lock employee computers after a period of inactivity.
5. Developing policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device.
6. Training employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:
 - a. Locking rooms and file cabinets where records are kept;
 - b. Not sharing or openly posting employee passwords in work areas;
 - c. Encrypting sensitive customer information when it is transmitted electronically via public networks;
 - d. Referring calls or other requests for customer information to designated individuals who have been trained in how the Utility safeguards personal data;
 - e. Reporting suspicious attempts to obtain customer information to designated personnel.
7. Regularly reminding all employees of the Utility's policy — and the legal requirement — to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms.
8. Developing policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions.
9. Imposing disciplinary measures for security policy violations.
10. Preventing terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.
11. Know where sensitive customer information is stored and store it securely. Make sure only authorized employees have access. For example:
 - a. Ensure that storage areas are protected against destruction or damage from physical hazards, like fire or floods.

- b. Store records in a room or cabinet that is locked when unattended.
 - c. When customer information is stored on a server or other computer, ensure that the computer is accessible only with a “strong” password and is kept in a physically-secure area.
 - d. Where possible, avoid storing sensitive customer data on a computer with an Internet connection.
 - e. Maintain secure backup records and keep archived data secure by storing it off-line and in a physically-secure area.
 - f. Maintain a careful inventory of the Utility’s computers and any other equipment on which customer information may be stored.
12. Take steps to ensure the secure transmission of customer information. For example:
- a. When transmitting credit card information or other sensitive financial data, use a Secure Sockets Layer (SSL) or other secure connection, so that the information is protected in transit.
 - b. If the Utility collects information online directly from customers, make secure transmission automatic. Caution customers against transmitting sensitive data, like account numbers, via email or in response to an unsolicited email or pop-up message.
 - c. If the Utility must transmit sensitive data by email over the Internet, be sure to encrypt the data.
13. Dispose of customer information in a secure way and, where applicable, consistent with the FTC’s Disposal Rule, www.ftc.gov/os/2004/11/041118disposalfrn.pdf. For example:
- a. Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If hiring an outside disposal company, conduct due diligence beforehand by checking references or requiring that the company be certified by a recognized industry group.
 - b. Burn, pulverize, or shred papers containing customer information so that the information cannot be read or reconstructed.
 - c. Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information.
14. Monitoring the websites of the Utility’s software vendors and reading relevant industry publications for news about emerging threats and available defenses.
15. Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information. Be sure to:
- a. Check with software vendors regularly to get and install patches that resolve software vulnerabilities;
 - b. Use anti-virus and anti-spyware software that updates automatically;
 - c. Maintain up-to-date firewalls, particularly if using a broadband Internet connection or allow employees to connect to the network from home or other off-site locations;
 - d. Regularly ensure that ports not used for Utility business are closed; and
 - e. Promptly pass along information and instructions to employees regarding any new security risks or possible breaches.

16. Using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information. It's wise to:
 - a. Keep logs of activity on the network and monitor them for signs of unauthorized access to customer information;
 - b. Use an up-to-date intrusion detection system to alert the Utility of attacks;
 - c. Monitor both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from the system to an unknown user; and
 - d. Insert a dummy account into each of the customer lists and monitor the account to detect any unauthorized contacts or charges.
17. Taking steps to preserve the security, confidentiality, and integrity of customer information in the event of a breach. If a breach occurs:
 - a. Take immediate action to secure any information that has or may have been compromised. For example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet;
 - b. Preserve and review files or programs that may reveal how the breach occurred;
 - c. If feasible and appropriate, bring in security professionals to help assess the breach as soon as possible.
18. Considering notifying consumers, law enforcement, and/or businesses in the event of a security breach. For example:
 - a. Notify consumers if their personal information is subject to a breach that poses a significant risk of identity theft or related harm;
 - b. Notify law enforcement if the breach may involve criminal activity or there is evidence that the breach has resulted in identity theft or related harm;
 - c. Notify the credit bureaus and other businesses that may be affected by the breach. See Information Compromise and the Risk of Identity Theft: Guidance for Your Business at www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.htm; and
 - d. Check to see if breach notification is required under applicable state law.