AUBURN WATER SYSTEM

Identity Theft Prevention Program

Effective October 20, 2008

I. PROGRAM ADOPTION

Auburn Water System developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. 16 C. F. R. § 681.2. This Program was developed with oversight and approval of the Auburn Water System Board of Directors. After consideration of the size and complexity of the Utility's operations and account systems, and the nature and scope of the Utility's activities, the Auburn Water System Board of Directors determined that this Program was appropriate for Auburn Water System and therefore approved this Program on DATE 2008.

II. PROGRAM PURPOSE AND DEFINITIONS

A. Fulfilling requirements of the Red Flags Rule

Under the Red Flag Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4. Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the creditor from Identity Theft.

B. Red Flags Rule definitions used in this Program

The Red Flags Rule defines "Identity Theft" as "fraud committed using the identifying information of another person" and a "Red Flag" as a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

According to the Rule, a municipal utility is a creditor subject to the Rule requirements. The Rule defines creditors "to include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors."

All the Utility's accounts that are individual utility service accounts held by customers of the utility whether residential, commercial or industrial are covered by the Rule. Under the Rule, a "covered account" is:

1. Any account the Utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and

2. Any other account the Utility offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Utility from Identity Theft.

"Identifying information" is defined under the Rule as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing code.

III. IDENTIFICATION OF RED FLAGS.

In order to identify relevant Red Flags, the Utility considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. The Utility identifies the following red flags, in each of the listed categories:

A. Notifications and Warnings From Credit Reporting Agencies

Red Flags

1) Report of fraud accompanying a credit report;
2) Notice or report from a credit agency of a credit freeze on a customer or applicant;
3) Notice or report from a credit agency of an active duty alert for an applicant; and
4) Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another customer;
6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and
8. A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

Red Flags

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use (example: very high activity);
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to the Utility that a customer is not receiving mail sent by the Utility;
6. Notice to the Utility that an account has unauthorized activity;
7. Breach in the Utility's computer system security; and
8. Unauthorized access to or use of customer account information.

E. Alerts from Others

Red Flag

1. Notice to the Utility from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

IV. DETECTING RED FLAGS.

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a **new account**, Utility personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
2. Verify the customer's identity (for instance, review a driver's license or other identification card);
3. Review documentation showing the existence of a business entity; and
4. Independently contact the customer.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an **existing account**, Utility personnel will take the following steps to monitor transactions with an account:

Detect

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Utility personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Mitigate

1. Continue to monitor an account for evidence of Identity Theft;
2. Contact the customer;
3. Change any passwords or other security devices that permit access to accounts;
4. Not open a new account;
5. Close an existing account;
6. Reopen an account with a new number;

7. Notify the General manager for determination of the appropriate step(s) to take;
8. Notify law enforcement; or
9. Determine that no response is warranted under the particular circumstances.

Protect customer identifying information

In order to further prevent the likelihood of identity theft occurring with respect to Utility accounts, the Utility will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing customer information;
3. Ensure that office computers are password protected and that computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer information;
5. Request only the last 4 digits of social security numbers (if any);
6. Ensure computer virus protection is up to date; and
7. Require and keep only the kinds of customer information that are necessary for utility purposes.

VI. PROGRAM UPDATES

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the Utility from Identity Theft. At least on a yearly basis, the Auburn Water System Board of Directors will consider the Utility's experiences with Identity Theft situation, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the Utility maintains and changes in the Utility's business arrangements with other entities. After considering these factors, the general manager will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the general manager will present to the Auburn Water System Board of Directors with his or her recommended changes and the Board will make a determination of whether to accept, modify or reject those changes to the Program.

VII. PROGRAM ADMINISTRATION.

A. Oversight

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee for the Utility. The Committee is headed by the general manager who may be the head of the Utility or his or her appointee. Two or more other individuals appointed by the head of the Utility or the general manager comprise the remainder of the committee

membership. The general manager will be responsible for the Program administration, for ensuring appropriate training of Utility staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports

Utility staff responsible for implementing the Program shall be trained either by or under the direction of the general manager in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

C. Service Provider Arrangements

In the event the Utility engages a service provider to perform an activity in connection with one or more accounts, the Utility will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review the Utility's Program and report any Red Flags to the general manager.

D. Specific Program Elements and Confidentiality

For the effectiveness of Identity Theft prevention Programs, the Red Flag Rule envisions a degree of confidentiality regarding the Utility's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices are to be limited to the Identity Theft Committee and those employees who need to know them for purposes of preventing Identity Theft. Because this Program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program's general red flag detection, implementation and prevention practices are listed in this document.

Approved this 20th day of October, 2008

_____

Donald Cadenhead-President

_____

Brenda Smith-Secretary

Appendix

Risk Assessment

Auburn Water System 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 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):

Auburn Water System 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:

- 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:
    - Recent and significant increase in volume of inquiries
    - Unusual number of recent credit applications
    - A material change in use of credit
    - 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.

- ❑ 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

Appendix A

Other Security Procedures

The following suggestions are not part of or required by the Federal Trade Commission's "Identity Theft Red Flags Rule". The following is a list of other security procedures a utility should consider to protect consumer information and to prevent unauthorized access. Implementation of selected actions below according to the unique circumstances of utilities is a good management practice to protect personal consumer data.

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. User names and passwords will be different.

26. Passwords will be changed at least monthly.

27. Passwords will not be shared or posted near workstations.

28. Password-activated screen savers will be used to lock employee computers after a period of inactivity.

29. When installing new software, vendor-supplied default passwords are changed.

30. The use of laptops is restricted to those employees who need them to perform their jobs.

31. Laptops are stored in secure place.

32. Laptop users will not store sensitive information on their laptops.

33. Laptops which contain sensitive data will be encrypted

34. Employees never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage.

35. If a laptop must be left in a vehicle, it is locked in a trunk.

36. The computer network will have a firewall where your network connects to the Internet.

37. Any wireless network in use is secured.

38. Maintain central log files of security-related information to monitor activity on your network.

39. Monitor incoming traffic for signs of a data breach.

40. Monitor outgoing traffic for signs of a data breach.

41. Implement a breach response plan.

42. Check references or do background checks before hiring employees who will have access to sensitive data.

43. New employees sign an agreement to follow your company's confidentiality and security standards for handling sensitive data.

44. Access to customer's personal identify information is limited to employees with a "need to know."

45. Procedures exist for making sure that workers who leave your employ or transfer to another part of Auburn Water System no longer have access to sensitive information.

46. Implement a regular schedule of employee training.

47. Employees will be alert to attempts at phone phishing.

48. Employees are required to notify the general manager immediately if there is a potential security breach, such as a lost or stolen laptop.

49. Employees who violate security policy are subjected to discipline, up to, and including, dismissal.

50. 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.

51. Paper records will be shredded before being placed into the trash.

52. 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.

53. Any data storage media will be disposed of by shredding, punching holes in, or incineration.

SENSITIVE and NON-PUBLIC INFORMATION GUIDELINE

1. PURPOSE

Auburn Water System adopts this policy to help protect employees, customers, contractors, and Auburn Water System from damages related to loss or misuse of sensitive information. This policy will:

- Define sensitive information
- Describe the physical security of data when it is printed on paper
- Describe the electronic security of data when stored and distribute

2. SCOPE

This policy applies to employees, contractors, consultants, temporaries, and other workers at Auburn Water System, including all personnel affiliated with third parties.

3. GUIDELINE

3.1. Definition of Sensitive Information

Sensitive information includes the following items whether stored in electronic or printed format:

3.1.1. Personal Information – Sensitive information consists of personal information including, but not limited to:

3.1.1.1. Credit Card Information, including any of the foI1owing:

- Credit Card Number (in part or whole)
- Credit Card Expiration Date
- Cardholder Name
- Cardholder Address

3.1.1.2. Tax Identification Numbers, including:

- Social Security Number
- Social Insurance Number
- Business Identification Number
- Employer Identification Numbers

3.1.1.3. Payroll information, including, among other information:

- Pay checks
- Pay stubs
- Pay rates

3.1.1.4. Cafeteria Plan Check Requests and associated paperwork

3.1.1.5. Medical Information for any Employees or Customers, including but not limited to:

- Doctor names and claims
- Insurance claims
- Prescriptions
- Any related personal medical information

3.1.1.6. Other Personal Information belonging to Customers, Employees and Contractors, examples of which include:

- Date of Birth
- Address
- Phone Numbers
- Maiden Name
- Names
- Customer Number

3.1.2. Corporate Information- Sensitive corporate information includes, but is not limited to:

3.1.2.1. Company, employee, customer, vendor, supplier confidential, proprietary information or trade secrets.

3.1.2.2. Proprietary and/or confidential information, among other things, includes: business methods, customer utilization information, retention information, sales information, marketing and other Company strategy, computer codes, screens, forms, information about, or received from, Company's current, former and prospective customers, sales associates or suppliers or any other non- public information. Proprietary and/or confidential information also includes the name and identity of any customer or vendor and the specifics of any relationship between and among them and Auburn Water System. .

3.1.3. Any document marked "Confidential," "Sensitive," "Proprietary," or any document similarly labeled.

3.1.4. Auburn Water System personnel are encouraged to use common sense judgment in securing Auburn Water System confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor/manager.

3.2. Hard Copy Distribution

Every employee and contractor performing work for Auburn Water System will comply with the following policies:

3.2.1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.

3.2.2. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday.

3.2.3. Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use.

3.2.4. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.

3.2.5. When documents containing sensitive information are discarded they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut or Department of Defense (DOD) approved shredding device. Locked shred bins are labeled *"Confidential paper shredding and recycling"*. If you need any assistance in locating one of these bins, please contact a supervisor/manager.

3.3. Electronic Distribution

Every employee and contractor performing work for Auburn Water System will comply with the following policies:

3.3.1. Internally, sensitive information may be transmitted using approved company email. All sensitive information must be encrypted when stored in an electronic format.

3.3.2. Any sensitive information sent external must be encrypted and password protected and only to approved recipients. Additionally, a statement such at this should be included in the email,

"This message may contain confidential and/or proprietary information, and is intended for the person/entity to *which it was originally addressed. Any use by others is strictly prohibited."*

4. ROLES AND RESPONSIBILITIES

Management will have the responsibility to enforce this policy and ensure that employees and contractors follow it.

5. DEFINITIONS

Encryption The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain test.

Hard Copy A printout of data stored in a computer. It is considered hard because it exists physically on paper, whereas a soft copy exists only electronically.

6. ENFORCEMENT

Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.