RESOLUTION NO. 5690

A RESOLUTION ADOPTING THE IDENTITY THEFT PROTECTION POLICY FOR THE CITY OF ALBANY.

WHEREAS, on March 4, 2008, the City Manager and Finance Director signed an Identify Theft Protection Policy to safeguard personally identifiable information and to comply with Senate Bill 583, the Oregon Identity Theft Protection Act (OITPA); and

WHEREAS, the policy placed responsibility on department directors to become familiar with the requirements of the act and to train employees in safeguarding protected information; and

WHEREAS, in September 2008, the League of Oregon Cities distributed a notice that cities that provide utility services would be subject to the Federal Trade Commission (FTC) "Red Flag" rules; and

WHEREAS, the FTC rules broaden the safeguards included in the City's Identify Theft Protection Policy and include requirements for specific operations where personal information is collected; and

WHEREAS, the Red Flag rules require that governing boards adopt a formal policy by November 1, 2008; and

WHEREAS, the attached policy combines the previous Identify Theft Protection Policy with the FTC Red Flag rules.

NOW, THEREFORE, BE IT RESOLVED that the City of Albany City Council hereby adopts Exhibit A as the Identity Theft Protection Policy for the City of Albany; and

BE IT FURTHER RESOLVED that the City Manager is directed to implement the policy and provide for the required annual review.

DATED AND EFFECTIVE THIS 22ND DAY OF OCTOBER, 2008.

Mayor

ATTEST:

City Clerk

G:\Mary\Resolutions & Ordinances\Identity Theft Protection Policy.docx

	City of Albany Finance Policy Policy #: F-04-08-002 Title: Identity Theft Protection Policy	**Exhibit A**

Purpose

To outline procedures for compliance with Senate Bill 583, the Oregon Identity Theft Protection Act (OITPA) and Federal Trade Commission (FTC) Code of Federal Regulations (CFR) 16 CFR Part 681 – Identity Theft Rules.

Scope

This policy applies to all employees.

Policy

It is the policy of the City of Albany to protect identifying information and comply with the OITPA and FTC 16 CFR Part 681 – Identity Theft Rules.

Resolution No. ____ establishes the Identity Theft Protection policy.

This policy is used in conjunction with two additional guidance documents:

- Identify Theft – A Business Guide
  http://10.1.20.123/phpsmb/browse.php?dir=%2FShared%2FIntranet%2FFinance%2FPolicies%2F&file=Identity+Theft+-+A+Business+Guide.pdf
- Identify Theft – Red Flags
  http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf
  (pages 63771 – 63774)

Guidelines

1. **Safeguarding Identifying Information**: The City of Albany shall implement and maintain reasonable safeguards to protect Identifying Information, which is defined as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person", such as: name, address, telephone number, social security number (SSN), date of birth, driver's license or identification card, alien registration number, employer or taxpayer identification number, unique electronic identification number, computer internet protocol address, or routing code.

2. **Social Security Number Protection**: Printing SSNs on any mailed materials not requested by the employee or customer unless redacted; or on cards used to access products, services, or City buildings (such as ID cards); or publicly posting or displaying SSNs is prohibited. Exemptions include requirements by the state of Oregon; federal laws including documents such as W2s, W4s, 1099s, etc; records that are

required by law to be made available to the public; records for use for internal verification or administrative processes; and records used for enforcing a judgment or court order.

3. **Red Flag Program Requirements:** "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft. Departments must develop and implement a written program that includes the following elements:
   a. Identify relevant Red Flags for the covered accounts maintained by the City;
   b. Detect Red Flags that have been incorporated into the procedure;
   c. Respond appropriately to any red Flags that are detected to prevent and mitigate identity theft; and
   d. Review the program annually to reflect changes in risks and evaluate the protections in place.

   Examples of Red Flags are identified in Supplement A to Appendix A of FTC 16 CFR Part 681 (pages 63771 – 63774), at the following link: http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf

4. **Notification of Security Breach**: In the event that personal identifying information has been subject to a security breach, the City will provide notification of the breach to the customer or the employee as soon as possible in writing, or electronically if that is the primary manner of communication with the customer or employee, or by telephone if the person is contacted directly. The exception is if the notification would impede a criminal investigation.

Responsibility

1. **Information Technology Department (IT)**: IT is responsible to establish technical controls to safeguard personal information stored in electronic format and to document safeguard practices in writing.

2. **Human Resources Department (HR):** HR is responsible to include this Identity Theft Protection Policy as part of new employee orientation by documenting review of this policy and the concepts in "Identity Theft – A Business Guide", located on the Intranet at: http://10.1.20.123/phpsmb/browse.php?dir=%2FShared%2FIntranet%2FFinance%2FPolicies%2F&file=Identity+Theft+-+A+Business+Guide.pdf

3. **Department Directors:** Department Directors are responsible to be familiar with the Identity Theft Protection Act and must develop and implement a written internal program that includes Red Flag requirements for their department. The internal program must be reviewed by the director annually.

   Department directors are also responsible to include this policy in temporary employee orientation by documenting review of this policy and the concepts in "Identity Theft – A Business Guide".

4. **Employees:** Employees are responsible to comply with this policy and any internal processes as directed by their department. Noncompliance may result in formal disciplinary action up to and including termination of employment. Employees should contact their supervisor if they have questions about compliance with this policy.

Supercedes: F-04-08-001	Created/Amended: Mar 4, 2008/Oct 22, 2008	Effective Date: November 1, 2008

American Water Works Association

The Authoritative Resource on Safe Water®

Utility Member Benefit

Government Affairs Office
1300 Eye Street NW
Suite 701W
Washington, DC 20005
T 202.628.8303
F 202.628.2846

Headquarters
6666 West Quincy Avenue
Denver, CO 80235-3098
Washington, DC 20005
T 303.794.7711
F 303.795.1989
www.awwa.org

Regulatory Alert

To: AWWA Utility Members

From: AWWA Government Affairs

Date: October 23, 2008

Who:	**Federal Trade Commission**
What:	**Change in date for utilities to be responsible for having a written program in place to help prevent identity theft**
When:	**Enforcement delayed to May 1, 2009**

The Federal Trade Commission (FTC) has announced it will grant a six-month delay of enforcement of the "Red Flags" rule until May 1, 2009. This rule will require creditors and financial institutions to establish identify theft prevention programs that identify and detect warning signs, also known as "Red Flags," of identify theft. Utilities and a host of other businesses and institutions in the United States previously had until November 1, 2008, to have a written program in place.

The FTC also today released an Enforcement Policy Statement, available at http://www.ftc.gov/os/2008/10/081022idtheftredflagsrule.pdf, which further details the rationale behind this delay of enforcement. In summary, the FTC learned during outreach efforts that some entities and industries were uncertain about their coverage and responsibilities under the rule, and postponed enforcement to allow greater education and compliance.

Examples of Red Flags include unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The FTC has listed 26 possible Red Flags.

The program was created in the Fair and Accurate Credit Transactions Act of 2003. While the bill does not mention utilities specifically, it says the Red Flag program applies to "financial

institutions" and "creditors" with "covered accounts." The FTC has determined that a creditor is "any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit."

An FTC rule notice further states that creditors include "utility companies," and that "where non-profit and government entities defer payment for goods and services, they, too, are to be considered creditors." A "covered account is an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions." The FTC further says that "utility accounts" are covered accounts. The notice is at http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm.

Questions about the rule may be directed by e-mail to RedFlags@ftc.gov.

# # #