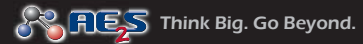


The Source

UTILITY ENTERPRISE MANAGEMENT

4th Quarter 2008



2009 Intended Use Plans

The Minnesota Public Facilities Authority (PFA) has approved its 2009 Intended Use Plans (IUPs) for the Clean Water Revolving Fund (CWRF) and the Drinking Water Revolving Fund (DWRF). The IUPs list water and wastewater projects that are eligible to receive loans from the PFA in FY09. A complete loan application must be submitted to the PFA to maintain eligibility. Plans and specifications must be submitted to the Health Department (for water projects) and to the Minnesota Pollution Control Agency (MPCA) (for wastewater projects) no later than March 2, 2009.

Loan application forms, as well as supplemental materials, have been substantially revised. The new forms and instructions, as well as a list of the approved IUPs are available on the PFA's website www.deed.state.mn.us/community/assistance/pfa.htm.

The United States Environmental Protection Agency (USEPA) has adopted new Disadvantaged Business Enterprise (DBE) regulations which will apply to all CWRF and DWRF projects. A contract packet, which is available at the PFA web site listed above, must be incorporated into all plans and specifications submitted to the MPCA or Health Department. ■

Minnesota Conservation Rate Requirements

Effective January 1, 2010, all Metro public water suppliers in Minnesota (serving over 1,000 people) must adopt a conservation

(continued on back)

Identify theft has become a growing and well-publicized problem in recent years. The Federal Trade Commission issued Identity Theft Red Flag and Address Discrepancy regulations under the Fair and Accurate Credit Transaction Act of 2003 (FACTAct) on November 9, 2007, requiring financial institutions and creditors with covered accounts to implement a written Identity Theft Prevention Program by November 1, 2008. These regulations, published in the November 9, 2007, Federal Register, are commonly referred to as the "Red Flag Rules". Utility companies fall under the definition of "creditor with covered

Utilities Required to Comply with FACTAct by November 1, 2008

accounts" and are subject to fines for noncompliance regardless of size and governmental status. The

regulation is intended to help protect consumers from fraud and identity theft by identifying and responding to potential red flags in a timely manner. In addition, utilities that use credit reports are subject to address discrepancy rules. Although not discussed in this article, the address discrepancy rules, in short, require a utility to make a good faith effort to verify customer addresses when notified of a discrepancy through a credit report.

This article discusses the Red Flag Rules portion of the regulation. There are four main components of the Red Flag Rules: identify relevant red flags, detect red flags, prevent and mitigate identity theft, and administer the program. The following steps ensure compliance with the four requirement elements:

- 1. Identify potential red flags.** Each utility must compile a list of red flags that are specifically pertinent to their operations. Examples of red flags are: notification or warning from a consumer reporting agency, address discrepancy when credit report is pulled, suspicious account activity (odd address change, irregular behavior within the account), suspicious documents, personal identifying information associated with prior fraud, or notification by the customer.
- 2. Develop procedures for detecting red flags.** Specific procedures need to be adopted to detect red flags in daily operations. For example, each entity needs to decide who is responsible for verifying initial customer information, what items are acceptable forms of identification and address verification, etc. Additionally, an individual must be chosen to monitor the program and to ensure ongoing red flag identification.
- 3. Establish Procedures for the Appropriate Response to Red Flags.** A party responsible for responding to a red flag must be appointed, and procedures to be followed subsequent to red flag identification must be outlined. Examples of specific responses include, but are not limited to, cancelling the transaction, notifying law enforcement, determining the extent of the entity's liability in the situation, and/or notifying the customer that a fraudulent incident either occurred or was attempted.
- 4. Establish procedures to effectively oversee service providers.** Monitoring procedures must be determined to ensure service providers and third party vendors are following the requirements of FACTAct. This may include reviewing the vendors' written policies, interviewing utility employees, etc.
- 5. Establish a written program.** Policies and procedures must be documented and made available for employee reference. Sensitive information should be defined in the program (i.e. credit card information, social security numbers,

(continued on back)

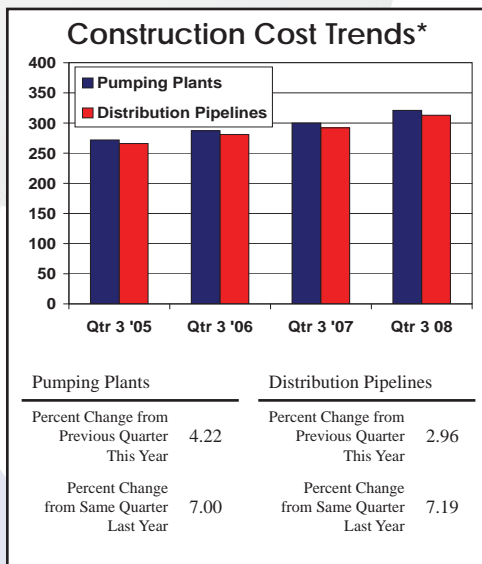
(MN Rates continued from first page)

rate structure; by January 1, 2013 all Non-Metro (serving over 1,000 people) must comply. Examples of the required conservation rates include increasing block rates, seasonal rates, excess use rates, time of use rates, and individual goal rates. Look for more information regarding this statute in upcoming issues of *The Source*. ■

(FACTAct Compliance continued from first page)

medical information, date of birth, maiden names, addresses, phone numbers, and customer numbers). Complete and ongoing measures for securing both hard and electronic versions of this information must be identified (such as keeping locked filing cabinets, removing social security numbers from account information, requiring identification at account opening, secure internet access both into and out of the entities system, clean desk policies, and locked storage rooms). Risks imposed on the entity as well as the entity's customers need to be identified (i.e. financial and reputational risks). Red flags, resolutions, and responsibilities as discussed in Items 1-4 must also be documented. The program should contain a training schedule with a synopsis of the information covered.

6. **Obtain approval of the written program by the appropriate governing body.** The governing body should review and approve the written policy annually. The entire staff is responsible for compliance with FACTAct; however, one person should be appointed to administer the program. Typical choices for the program administrator are City Recorders, Finance Directors, or IT Directors.
7. **Train staff.** In order to provide for an effective program, staff needs to be trained on the necessity of the regulation and the procedures established. Training should cover the written policy as well. Pertinent staff should be included, erring on the side of caution when selecting personnel to attend the training.
8. **Provide for continuing oversight of the program.** The program and written policy should be dynamic and evolve as necessary as identity theft becomes more sophisticated. At a minimum, this program should be updated annually.



*Based on information from the Bureau of Reclamation

The examples provided above are not all inclusive and each utility must address each step as it relates to its specific situation. Overall, the program should be tailored to the size and complexity of the utility. If you have questions regarding FACTAct compliance, or would like assistance in creating your program, contact JoDee Hass at (701) 746-8087 or JoDee.Hass@ae2s.com. ■

www.ae2s.com

Offices in:
Grand Forks, ND
Bismarck, ND
Williston, ND
Fargo, ND
Moorhead, MN
Minneapolis, MN
Great Falls, MT

Advanced Engineering and Environmental Services, Inc. (AE2S)
2016 Washington Street South
Grand Forks, ND 58201