

## **New “Red Flag” requirements apply to water utilities**

**Red Flag Rules Update** – It has become apparent that water utilities will be required to comply with the FTC’s Red Flag (identity theft prevention) Rule by November 2008. As of September 4, 2008, the National Rural Water Association in Washington is drafting a compliance template for all systems to use for compliance. The initial thought is to have the compliance template on one internet site that anyone can use to easily, simply, and economically comply with the rule in short order.

### **What’s all this new stuff about “Red Flag”?**

Identity thieves use people’s personally identifying information to open new accounts and misuse existing accounts, creating havoc for consumers and businesses. Financial institutions and creditors soon will be required to implement a program to detect, prevent, and mitigate instances of identity theft.

The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations (the Red Flags Rules) requiring financial institutions and creditors to develop and implement written identity theft prevention programs, as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. The programs must be in place by November 1, 2008, and must provide for the identification, detection, and response to patterns, practices, or specific activities — known as “red flags” — that could indicate identity theft.

### **Who must comply with the Red Flags Rules?**

The Red Flags Rules apply to “financial institutions” and “creditors” with “covered accounts.”

Under the Rules, a financial institution is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a “transaction account” belonging to a consumer. Most of these institutions are regulated by the Federal bank regulatory agencies and the NCUA. Financial institutions under the FTC’s jurisdiction include state-chartered credit unions and certain other entities that hold consumer transaction accounts.

A transaction account is a deposit or other account from which the owner makes payments or transfers. Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

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. Accepting credit cards as a form of payment does not in and of itself make an entity a creditor. Creditors 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. Most creditors, except for those regulated by the Federal bank regulatory agencies and the NCUA, come under the jurisdiction of the FTC.

A covered account is an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts. A covered account is also an account for which there is a foreseeable risk of identity theft – for example, small business or sole proprietorship accounts.

### **Complying with the Red Flags Rules**

Under the Red Flags Rules, financial institutions and creditors must develop a written program that identifies and detects the relevant warning signs – or “red flags” – of identity theft. These may include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The program must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the program. The program must be managed by the Board of Directors or senior employees of the financial institution or creditor, include appropriate staff training, and provide for oversight of any service providers.

## **How flexible are the Red Flags Rules?**

The Red Flags Rules provide all financial institutions and creditors the opportunity to design and implement a program that is appropriate to their size and complexity, as well as the nature of their operations. Guidelines issued by the FTC, the federal banking agencies, and the NCUA ([ftc.gov/opa/2007/10/redflag.shtm](http://ftc.gov/opa/2007/10/redflag.shtm)) should be helpful in assisting covered entities in designing their programs. A supplement to the Guidelines identifies 26 possible red flags. These red flags are not a checklist, but rather, are examples that financial institutions and creditors may want to use as a starting point. They fall into five categories:

- alerts, notifications, or warnings from a consumer reporting agency;
- suspicious documents;
- suspicious personally identifying information, such as a suspicious address;
- unusual use of – or suspicious activity relating to – a covered account; and
- notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts.

For more information visit our website at [www.okruralwater.org](http://www.okruralwater.org).