"IDENTITY THEFT" AND MUNICIPAL UTILITIES

Identity Theft and Red Flags Rule requirements

The Red Flags Rule implements portions of the Fair and Accurate Credit Transactions Act of 2003 (FACTA). Section 111 of FACTA defines "Identity Theft" as "fraud committed using the identifying information of another person."

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

- Identify relevant Red Flags for new and existing "covered accounts" (defined below) and incorporate those Red Flags into the Program;
- Detect Red Flags that have been incorporated into the Program;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
- 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.

The Rule requires the Program to be approved by "a designated employee at the level of senior management."

Definitions related to municipal utilities

According to the Rule, a municipal utility is a creditor subject to the Rule requirements. Accounts maintained by a municipal utility that are covered by the Rule are all the individual utility service accounts held by customers of the utility whether residential, commercial or industrial.

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."

Under the Rule, a "covered account" is:

- Any account the Utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
- 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." It specifically includes all of the items listed below.

- 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
- Routing code

The tables on the following two pages are intended as tools to assist your Identity Theft Prevention Committee in identifying specific Red Flags and procedures at your utility for incorporation into your utility employee training and, as desired, your written Identity Theft Prevention Program. The items in each table may be used to generate discussion about Identity Theft threats and prevention and ought to be modified, expanded or refined as necessary.

"IDENTITY THEFT" (FRAUD) TYPE 1 – NEW ACCOUNTS

❒ Establishing utility service using another person's identity

Why would someone do it?

- The perpetrator defaulted on a past utility account or other account and so would not be eligible for service under his or her own name.
- The perpetrator intends to establish fraudulent proof of residency in order to commit fraud elsewhere.

Red flag:	**Detect whether fraud is being attempted or committed:**	**Prevent or mitigate detected fraud:**
ID picture doesn't match person	Request additional ID	Do not open account
ID information doesn't match person	Request additional ID	Do not open account
ID does not look authentic	Request additional ID	Do not open account
ID looks doctored	Request additional ID	Do not open account
Using a suspicious name	Request additional ID	Do not open account
Applicant requests that bill be sent to address different from where service is received	Verify that customer is connected to billing address (But be aware of the state's "Safe at Home" program)	Do not open account
Account for a residential address established under business name (to avoid using own bad name)	Obtain credit report on the individual	Do not open account
Credit report contains fraud warning, credit freeze notice or active duty alert	This may be an automatic fraud detection Red Flag	Notify Program Administrator; If warranted, notify law enforcement
Bill payment made under name other than that on utility account	Request proof of residence (other bills, etc.)	Close account
Other?		
Other?		
Other?		

"IDENTITY THEFT" (FRAUD) TYPE 2 – EXISTING ACCOUNTS

❒ Continuing utility service under a another customer's name after he or she moves out

Why would someone do it?

- The perpetrator wants to avoid paying for service.
- The perpetrator defaulted on a past utility account or other account and so would not be eligible for service under his or her own name.

Red flag:	**Detect whether fraud is being committed:**	**Mitigate detected fraud:**
Non-payment of previously current account	Call customer phone number on file	Discontinue service; close account
Utility service utilized after known move-out with no change of customer notice received by utility	Call customer phone number on file	Discontinue service; close account
Bill payment made under a name other than name on utility account	Call customer phone number on file	Discontinue service; close account
Other?		
Other?		
Other?		

MEMORANDUM

To: All MMUA Member Utilities

From: Bill Black, Government Relations Representative

Date: Aug 29, 2008

Re: Red Flags Rule guidance for municipal utilities

On August 4, MMUA sent a memo to all member utilities alerting them to an upcoming deadline set by the Federal Trade Commission (FTC) by which all utilities would be required to have an Identity Theft Prevention Program developed and in place. MMUA is committed to helping all member utilities meet that federal requirement.

What to do:

1) Go to: http://www.mmua.org.
2) Download the Identity Theft Prevention Program Template provided by MMUA.*
3) Assign a Program Administrator (Utility Manager or delegate).
4) Program Administrator: Appoint and lead an Identity Theft Prevention Committee including at least two additional responsible individuals (e.g., administrative director or information technician at your utility or the Administrator, Data Practices Compliance Officer or Attorney for your city).
5) Committee: Discuss and customize the program template to fit your utility's size and administrative practices following guidance provided on the following two pages.

* MMUA thanks Municipal Electric Utilities of Wisconsin for its assistance in developing the program template provided by MMUA.

GUIDANCE FOR COMPLYING WITH THE RED FLAGS RULE

Adoption of an Identity Theft Prevention Program

Your Identity Theft Prevention Program must be approved by either your governing commission or council **OR BY A DESIGNATED EMPLOYEE AT A SENIOR LEVEL OF MANAGEMENT** by November 1, 2009. The Federal Trade Commission will not be checking individual utilities to see if this deadline is met, however, so failure to meet it should not be considered urgent. Having a well thought-out program in place in the near future is preferred to incorporating a pro-forma plan "for the books." ***The Federal Trade Commission currently says it is further extending its deferral of enforcement of the Identity Theft Red Flags Rule to November 1, 2009.***

Customizing a template for your utility

The template provided by MMUA should be modified as necessary to fit your utility. You may also find useful information in the document "Identity Theft and Municipal Utilities" provided by MMUA through its website.

The Red Flags Rule is meant to prevent "Identity Theft" as the Rule defines it – fraud using another person's identifying information. While the theft of customer identification information may lead to "Identity Theft," information theft itself is not the focus of the Rule. Also keep in mind that the Federal Trade Commission created this rule particularly with banks, credit card providers and large private utilities in mind. While significant, the types of fraud encountered at utilities, particularly smaller utilities, are more limited in nature. (See MMUA's "Identity Theft and Municipal Utilities.")

Note that some smaller utilities may not find it necessary to use certain Identity Theft prevention techniques included in the template, such as requiring photo ID for new accounts. While the Red Flags categories and Red Flags themselves in the template are examples taken nearly directly from FTC-provided information, your utility must determine the specific items to include, exclude or expand upon within each section. For instance, if you do not check credit reports, the first category under "Identification of Red Flags" may be eliminated altogether.

Your utility may find it useful to expand certain sections of the template. For example, the "Prevent and Mitigate Identity Theft" section may be drafted to show a range of possible responses to Red Flag detections and identify one or more persons who will be responsible within your utility for determining what response is appropriate depending upon circumstances. If the Utility receives notice that its system has been compromised such that a customer's personal information has become accessible, the Utility would likely, at a minimum, notify the customer and change passwords. If the Utility receives notice that a person has provided inaccurate identification information, the appropriate response may be to close the account and contact law enforcement. (See MMUA's "Identity Theft and Municipal Utilities" for further illustration.)

Other relevant laws

As you implement your utility's program, it may be useful to find out more about certain laws that could potentially affect it, particularly these:

Federal Privacy Act – Prohibits all federal, state and local government agencies from denying an individual any right, benefit or privilege provided by law because of such individual's refusal to disclose his or her social security number. (5 U.S.C. §552a note.)

Minnesota's Government Data Practices law – Requires government entities to appoint or designate an employee of the government entity to act as its data practices compliance official and categorizes municipal electric utility individual customer information as "private data" and business or other entity customer data as "nonpublic." (Minn. Stat. Ch. 13.)

Minnesota's Safe at Home Program – Provides people who are at particular risk of certain abuse and harassment dangers with an alternative address and mail forwarding service for their protection. (Minn. Stat. Ch. 5B.)

[Utility Name]

Identity Theft Prevention Program

Effective beginning _____, 2009

I. PROGRAM ADOPTION

The [Utility Name] ("Utility") 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 [Program Administrator (defined below) OR ____Utility Commission OR ____City Council]. 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 [Program Administrator OR____Utility Commission OR ____City Council] determined that this Program was appropriate for the [Utility Name], and therefore approved this Program on _____, 2009.

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 Program Administrator 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 [Insert time: every 6 months, year, etc.], the Program Administrator 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 Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program or present the [Utility Commission OR City Council] with his or her recommended changes and the [Utility Commission OR City Council] 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 a Program Administrator 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 Program Administrator comprise the remainder of the committee membership. The Program Administrator 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 Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. *(The Utility may include in its Program how often training is to occur. The Program may also require staff to provide reports to the Program Administrator on incidents of Identity Theft, the Utility's compliance with the Program and the effectiveness of the Program.)*

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 Program Administrator.

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.