



MEMORANDUM

DATE: October 20, 2008

TO: All Cities

FROM: Kristin N. Eick
Phil A. Olbrechts

RE: FACTA Red Flag Guidelines

The Federal Trade Commission has issued regulations requiring financial institutions and creditors to develop and implement written identity theft prevention programs by November 1, 2008, under the Fair and Accurate Credit Transaction Act of 2003 (FACTA). Municipal utilities are subject to these requirements, and the City Councils of all cities that operate utilities must adopt programs that meet the requirements of FACTA. These identity theft prevention programs must provide for the identification, detection, and response to patterns, practices, or specific activities - known as "red flags" - that could indicate identity theft. Accompanying this memo is a sample program that complies with FACTA requirements.

Who must comply with FACTA?

Financial institutions and "creditors" that maintain "covered accounts," as defined in the Act, must comply with FACTA's Red Flag requirements. Under FACTA, a "creditor" means an entity that regularly extends, renews, or continues credit.¹ Non-profit and government entities are included within this definition of "creditor."² The Code of Federal Regulations establishes that the term "creditor" includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, *utility companies*, and telecommunications companies.³ "Credit" is defined in the Act as "the right granted by a creditor to a debtor to defer payment of debt or to incur debts

¹ 16 C.F.R. § 681.2(b)(5) (2008); 15 U.S.C. § 1681a(r)(5) (2006); 15 U.S.C. 1691a(e) (2006).

² Federal Trade Commission, FTC Business Alert, New "Red Flag" Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft, June 2008, *available at* <http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm>.

³ 16 C.F.R. § 681.2(b)(5) (emphasis added).

and defer its payment or to purchase property or services and defer payment therefor.”⁴ Therefore, essentially any business, whether public or private, that provides services and accepts payment later is considered a creditor if it maintains “covered accounts.”

“Covered accounts” include accounts that financial institutions or creditors offer or maintain primarily for personal, family, or household purposes, that involve or are designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, *utility account*, checking account, or savings account.⁵ The term “covered accounts” also includes any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, or litigation risks.⁶ Because “covered accounts” specifically include utility accounts, municipalities deferring payment for services such as water, electric, or garbage collection must comply with FACTA.

How do I comply with FACTA?

FACTA requires that municipalities, as creditors, develop a written Identity Theft Protection Program that is appropriate for the size and complexity of the municipality.⁷ The Program must include elements to identify, detect, and respond to Red Flags. In addition, the Program must provide for a periodic updating process to reflect changes in risks to the creditor’s customers.⁸

Each creditor is required to obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board, *i.e.*, the City Council.⁹ The board of directors, a committee of the board, or an employee at the level of senior management must be assigned the duties of oversight, development, implementation, and administration of the Program.¹⁰ Further, staff must be trained appropriately and must oversee service providers providing services relating to the Act.¹¹ Staff should prepare a report at least annually for the person specifically responsible for oversight of the program. This report should include an evaluation of the effectiveness of the Program with respect to opening accounts, existing covered accounts, service provider arrangements, significant incidents involving identity theft and responses, and recommendations for changes to the Program.¹²

What are “Red Flags?”

⁴ 16 C.F.R. § 681.2(b)(4); 15 U.S.C. 1681a(r)(5); 15 U.S.C. 1691a(d).

⁵ 16 C.F.R. § 681.2(b)(3)(i) (emphasis added).

⁶ 16 C.F.R. § 681.2(b)(3)(ii).

⁷ 16 C.F.R. § 681.2(d)(1).

⁸ 16 C.F.R. § 681.2(d)(2).

⁹ 16 C.F.R. § 681.2(e)(1).

¹⁰ 16 C.F.R. § 681.2(e)(2).

¹¹ 16 C.F.R. § 681.2(e)(3)-(4).

¹² 16 C.F.R. app. § 1681 A(VI)(b)(1).

Red Flags are patterns, practices, or specific activity that indicate the possible existence of identity theft.¹³ There are five general categories of Red Flags. The Federal Trade Commission has also provided a list of 26 suggested Red Flags in the appendix to the Code of Federal Regulations. The five categories are:

- Alerts or notifications from consumer reporting agencies or service providers, such as fraud detection services;
- Presentation of suspicious documents, such as identification documents that have been forged or altered;
- Presentation of suspicious personal identifying information, such as a suspicious address change or social security number;
- Unusual use of or other suspicious activity relating to a covered account, such as identification of use of an account in a manner inconsistent with established patterns of activity on the account; and
- Notices from customers, victims of identity theft, law enforcement, or other persons regarding identity theft in connection with covered accounts held by the creditor.¹⁴

Appropriate responses to Red Flags include:

- Monitoring an account;
- Contacting the customer;
- Changing passwords and security codes;
- Reopening an account with a new number;
- Not opening a new account;
- Closing an existing account;
- Notifying law enforcement; and
- Determining that no response is warranted under the particular circumstances.¹⁵

How is FACTA enforced?

FACTA does not allow for private enforcement of the Red Flag regulations. However, the regulations are enforced by the Federal Trade Commission.¹⁶ If the creditor fails to develop and implement a Program, the Federal Trade Commission may enforce the failure as an unfair or deceptive act or practice in commerce.¹⁷ The consequences may include a cease and desist order from the Federal Trade Commission after a hearing and civil penalties not to exceed \$2,500 per violation.¹⁸

¹³ 16 C.F.R. § 681.2(b)(9).

¹⁴ 16 C.F.R. Supplement A to App. § 1681 A.

¹⁵ 16 C.F.R. app. § 1681 A(IV).

¹⁶ 15 U.S.C. § 1681m(h)(8); *see also Perry v. First Nat'l Bank*, 459 F.3d 816, 819-20 (7th Cir. 2006).

¹⁷ 15 U.S.C. § 1681m(h)(8)(B); 15 U.S.C. § 1691s(a)(1).

¹⁸ 15 U.S.C. § 45(a)(1); § 45(b); § 1681s(a)(2)(A).

What Type of Program Must I Adopt?

Attached you will find a sample program that the City Council may adopt. It is important to remember, however, that the Red Flag Guidelines were designed to provide flexibility to the individual utility in adopting their Program. Because the process used to open new accounts and monitor existing accounts will vary by utility, not every Red Flag will be applicable to each utility. For example, the utility may not use credit reporting, and therefore, will not encounter Red Flags relating to consumer reports. Thus, the goal is to be aware of the Red Flags, remain vigilant in detecting those Red Flags that are applicable to a particular utility, and notify the Finance Director of the City if a Red Flag is encountered.

As most cities will readily observe, the Red Flags have little relevance to the billing practices of city utilities. The Federal Trade Commission, responsible for enforcement of FACTA, offers no guidance on how city utilities can implement these policies other than to suggest “common sense.” There is obviously little common sense in designating City utilities as “creditors” subject to FACTA. Implementing proactive measures to detect identity theft, such as comparing the names of all persons paying utility bills to the owners of property served, can be highly disruptive and costly to city operations. The recommended program minimizes costs as much as possible and is comparable to programs adopted throughout the country. More may be required of cities as court opinions and federal regulations further clarify the responsibilities of city utilities.

KNE:

[Utility Name]

Identity Theft Prevention Program

Effective beginning _____, 2008

I. PROGRAM ADOPTION

The [Utility Name] (“Utility”) developed this Identity Theft Prevention Program (“Program”) pursuant to the Federal Trade Commission's Red Flag 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 and approved by the 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 City Council determined that this Program was appropriate for the [Utility Name], and therefore adopted this Program on _____, 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 the size, complexity and 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 Flag 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 and will train appropriate staff to recognize these Red Flags as they are encountered in the ordinary course of Utility business:

A. Alerts, 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;
4. Notice or report from a credit agency of an address discrepancy; and
5. Indication from a credit report of activity that is inconsistent with a customer’s usual pattern or activity, such as an unusual increase in the volume of credit inquiries, unusual increase in the number of established credit relationships, or a material change in the use of credit.

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 information on identification document is not consistent with information provided by the person opening a new covered account, by the customer presenting the identification, or with existing customer information on file with the creditor (such as a signature card or recent check); 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, for instance, where there is a lack of correlation between the social security number range and the date of birth;
2. Identifying information presented that is inconsistent with external sources of information, for instance, an address does not match a consumer report or a social security number is listed in the Social Security Administration's Death Master File;
3. Identifying information presented is associated with common types of fraudulent activity, such as use of a fictitious billing address or phone number;
4. Identifying information presented that is consistent with known fraudulent activity, such as presentation of an invalid phone number or fictitious billing address used in previous fraudulent activity;
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. PREVENTING AND MITIGATING IDENTITY THEFT

In the event Utility personnel detect any identified Red Flags, such personnel must contact the Finance Director of the City. The Finance Director will then decide which of the following steps should be taken:

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 law enforcement; or
8. Determine that no response is warranted under the particular circumstances.

V. PROGRAM UPDATES

The [_____] shall serve as Program Administrator. The Program Administrator will periodically review and update this Program to reflect changes in risks to customers and the soundness of the Utility from Identity Theft. In doing so, the Program Administrator will consider the Utility's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, 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 City Council with his or her recommended changes and the 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 the Program Administrator. The Program Administrator will be responsible for the Program's administration, for ensuring appropriate training of Utility staff, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, for determining which steps of prevention and mitigation should be taken in particular circumstances, and for 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. Staff should prepare a report at least annually for the Program Administrator, including an evaluation of the effectiveness of the Program with respect to opening accounts, existing covered accounts, service provider arrangements, significant incidents involving identity theft and responses, and recommendations for changes to 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.