STATE OF TENNESSEE
COMPTROLLER OF THE TREASURY
OFFICE OF OPEN RECORDS COUNSEL
James K. Polk State Office Building
505 Deaderick Street, Suite 1600
Nashville, Tennessee 37243-1402

John G. Morgan
Comptroller

Ms. Tammy Dunn
Senior Staff Attorney
City of Oak Ridge
P.O. Box 1
Oak Ridge, Tennessee 37831

October 27, 2008

Ms. Dunn:

You have requested an opinion from this Office regarding the interplay and/or potential conflict between the Tennessee Public Records Act (hereinafter referred to as "TPRA") and the Identity Theft Red Flag Rules (hereinafter referred to as "Rules") that implement section 114 of the federal Fair and Accurate Credit Transactions Act of 2003 (hereinafter referred to as "FACTA"). Most Tennessee municipalities (including cities, counties and utility districts) meet the definition of "creditor" under FACTA by providing services (such as water and sewer services) to customers for which multiple payments are received (typically on a deferred basis).

It is the opinion of this Office that there is no conflict between the Rules and the TPRA because the Rules do not require governmental entities meeting the definition of "creditors" pursuant to FACTA to make any customer information confidential if other laws have not already made that information confidential,

I. An Overview of the Identity Theft Red Flag Rules

In November 2007, several federal agencies jointly issued what are commonly referred to as the Identity Theft Red Flag Rules which implement sections 114 and 315 of FACTA. Section 114 of FACTA, which is the section that is relevant to this opinion, required the Federal Banking Agencies, National Credit Union Administration, and the Federal Trade Commission (hereinafter jointly referred to as "Agencies") to do the following:

> (A) establish and maintain guidelines for use by each financial institution and each creditor regarding identity theft with respect to account holders at, or customers of, such entities, and update such guidelines as often as necessary; and
> (B) prescribe regulations requiring each financial institution and each creditor to establish reasonable policies and procedures for implementing the guidelines established pursuant to

subparagraph (A), to identify possible risks to account holders or customers or to the safety and soundness of the institution or customers.

In response to this directive the Agencies issued the Rules that became effective on January 1, 2008, and have a final compliance deadline of November 1, 2008. Definitions are provided to enable entities to determine whether or not they are subject to the Rules. Under the Rules it is only those "financial institutions" and "creditors" that offer and/or maintain "covered accounts" to "customers" that must establish and implement a written Identity Theft Prevention Policy.

The following definitions are important in determining what is required by the Rules and to whom the Rules apply.

"Account" is defined as:

(1) a continuing relationship established to obtain a product or service that an account holder may have with a financial institution; or
(2) creditor, which also includes an extension of credit, such as the purchase of property or services involving deferred payment.

Identity Theft Rules 16 C.F.R. §681.2(b)(1) (2008).

"Covered account" is defined as:

(1) an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions such as credit card accounts, utility accounts, checking and savings accounts, and mortgage loans; or
(2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft.

Identity Theft Rules 16 C.F.R. §681.2(b)(3) (2008) .

"Creditor" is defined as:

a person who arranges for the extension, renewal, or continuation of credit and includes lenders such as banks, finance companies, automobile dealerships, mortgage brokers, utility companies, and telecommunication companies.

Fair Credit Reporting Act 15 U.S.C. §1681A(r)(5) (2008) and Identity Theft Rules 16 C.F.R. §681.2(b)(5) (2008).

"Customer" is defined as:

a person that has a covered account with a financial institution or creditor.

Identity Theft Rules 16 C.F.R. §681.2(b)(6) (2008).

"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 person that, directly or indirectly, holds a transaction account (as defined in section 19(b) of the Federal Reserve Act) belonging to a consumer.

Fair Credit Reporting Act 15 U.S.C. §1681a(t) (2008).

"Identity theft" is defined as:

> a fraud committed or attempted using the identifying information of another person without permission.

Identity Theft Rules 16 C.F.R. §603.2(a) (2008) .

"Identifying information" is defined as:

> any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any-
>
> (1) Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
>
> (2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
>
> (3) Unique electronic identification number, address, or routing code; or
>
> (4) Telecommunication identifying information or access device [as defined in 18 U.S.C. §1029(e) (2008)].

Identity Theft Rules 16 C.F.R. §603.2(b) (2008).

These definition makes it is clear that most Tennessee municipalities (including cities, counties, and utility districts) are subject to Rules due to the fact that they provide to customers services that are primarily for personal or household purposes, and payment for such services is submitted in multiple payments (typically on a deferred payment basis).

So, the question becomes what is required of those entities that are subject to the Rules. Nothing within the Rules permits entities to make confidential any customer information that is not already made confidential by some other provision of law. The Rules address the procedures that entities must have in place that will allow them to identify, prevent, and mitigate identity theft related to transactions made with both new and existing accounts. Identity Theft Rules 16 C.F.R. §681.2(d) (2008)

In order to comply with the Rules, entities must first establish reasonable policies and procedures that identify as exhaustively as possible any "red flags" or practices, patterns, and specific activity that prompt suspicion that identity theft has occurred. Identity Theft Rules 16 C.F.R. §681.2(b)(9) (2008).

Next entities must establish reasonable policies and procedures that address how they will detect the red flags that were identified in the policies and procedures described above. In establishing policies and procedures on detecting red flags, the Rules suggest that when dealing with customers that are opening new accounts, entities should create procedures that incorporate obtaining identifying information about the customer opening the account and then verifying the information received. Identity Theft Rules 16 C.F.R. §681, app. § A (2008). When dealing with existing accounts, the Rules suggest that entities establish a method to authenticate they are actually talking to the person to whom the account belongs, monitor accounts for suspicious activity, and when change of address requests are received verify the authenticity of the requests. Identity Theft Rules 16 C.F.R. §861, app. § A (2008).

Entities must then establish reasonable policies and procedures that outline how the entities will respond appropriately to any red flag that is detected so that identity theft can be prevented and mitigated. Specific examples of what an appropriate response might entail include:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

Identity Theft Rules 16 C.F.R. §681, app. § A (2008).

Finally, entities subject to the Rules must establish reasonable policies and procedures to ensure that the entities' Identity Theft Prevention Programs are updated periodically to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor. So, as criminals find new ways to perpetrate identity theft, entities subject to the Rules must make sure that all policies and procedures established pursuant to the Rules are updated in response to newly identified methods of carrying out identity theft. 16 CF..R. §681, app. § A (2008).

II. The Interplay and/or Potential Conflict Between Policies and Procedure Established Pursuant to the Identity Theft Red Flag Rules and the Tennessee Public Records Act

The Rules make it clear that in implementing policies and procedures that will be used to detect, prevent, and mitigate identity theft, entities have broad latitude in establishing policies and procedures that are appropriate to the size, complexity and nature of the entities' operations; however, that latitude does not go so far as to allow entities to make confidential information not already made confidential by state or federal law. The Rules do not deal with the release of information, but rather how entities ensure that the customer information received for the purpose of opening a new account or used in connection with an existing account is authentic and has not been gained through identity theft.

There are a number of exceptions to the TPRA that make information that may be obtained by governmental entities from a "customer" with a "covered account" confidential. Several of the exceptions are set out below.

Tenn. Code Ann. Section 4-4-125 prohibits the public disclosure of social security numbers by state entities, unless the disclosure falls into one of the exceptions enumerated within the provision.

Tenn. Code Ann. Section 10-7-504(a)(15) creates an exception that requires confidentiality of certain identifying information that may be obtained by a utility service provider. This exception is specific to individuals who present a valid protection document to a utility service provider and request that his/her identifying information be kept confidential. The provision provides that any "identifying information," such as "home and work addresses and telephone numbers, social security numbers and any other information that could be used to locate the whereabouts of an individual" with a valid order of protection is confidential when in the possession of a utility service provider. Tenn. Code Ann. Section 10-7-504(a)(15)(A)(i). For purposes of this provision, "utility service provider" is defined as any entity, whether public or private, that provides electricity, natural gas, water, or telephone services to customers on a subscription basis, whether or not regulated by the Tennessee regulatory authority. Tenn. Code Ann. Section 10-7-504(a)(15)(A)(iii).

Additionally, Tenn. Code Ann. Section 10-7-504(a)(16) creates an exception to the TPRA that permits the State, any county, municipality, city, or political subdivision of the State to treat any identifying information that could reasonably be used to locate a person with a valid protection document as confidential.

Tenn. Code Ann. Section 10-7-504(a)(19) provides that the credit card numbers of persons doing business with the State or a political subdivision thereof and any related information such as PINs and authorization codes are confidential, whether the information is received through electronic means or a paper transaction.

Finally, Tenn. Code Ann. Section 10-7-504(a)(20)(A) provides that the "private records" or credit card numbers, social security numbers, tax identification numbers, bank account numbers, security codes, access codes, and burglar alarm codes associated with customers and customer accounts that are in possession of a public utility shall be treated as confidential. For purposes of this provision, "utility" is defined as:

> any public electric generation system, electric distribution system, water storage or processing system, water distribution system, gas storage system or facilities related thereto, gas distribution system, wastewater system, telecommunications system, or any services similar to the foregoing.

The Rules do not create a mechanism by which entities can make confidential customer information that is otherwise public. Unless a specific provision in law can be identified as creating an exception to the TPRA, identifying information associated with a customer is going to be open for personal inspection and copying by any citizen of Tennessee as long as that information was "made or received pursuant to law or ordinance or in connection with the transaction of official business by any governmental agency." Tenn. Code Ann. Section 10-7-503(a)(1), as amended by Public Chapter 1179, Acts of 2008.

III. Conclusion

For the above mentioned reasons, it is the opinion of this Office that there is no conflict between the TPRA and the Rules. The TPRA addresses a Tennessee citizen's right to access "public records." The Rules neither address public disclosure of customer identifying information nor suggest that the policies and procedures that are to be developed and implemented by the entities subject to the Rules address public disclosure of customer identifying information. The Rules require entities to establish and implement policies and procedures that assist in identifying, preventing and mitigating the use of identity theft with new and existing accounts; and that directive does not conflict with the TPRA.

Please feel free to call either myself or Ann V. Butterworth at (615) 401-7891 if you have any further questions.

Elisha D. Hodge
Open Records Specialist
Office of Open Records Counsel