FACING THE FACTA

THE RED FLAG RULE:
AN IDENTITY THEFT RISK AUDIT
for Municipal Lawyers

Presented to
IMLA Spring Conference
Washington, D.C.

April 2009

Diane Pedicord
General Counsel
Oklahoma Municipal League

The Red Flag Rule:
An Identity Theft Risk Audit
for Municipal Lawyers

Lawyers have an occupational hazard of seeing a tort waiting to happen where others only see something ugly or unpleasant or defective. When looking at the FACTA Red Flag Rule, it is appropriate, therefore, to ask whether this federal rule creates new risks of liability for our municipal clients. I submit that it does and that we should look beyond the Rule's penalties for noncompliance to other sources of liability stemming from its promulgation.

What is this Red Flag Rule? At Congress' direction, five federal agencies jointly issued rules to implement the Fair and Accurate Credit Transactions Act (FACTA). The purpose of the Act: to curb identity theft. The mandate: creditors must adopt and carry out an Identity Theft Prevention Program (ITPP) that contains each of the basic elements specified in the Red Flag Rule.

What is a Red Flag? It is a "pattern, practice, or specific activity that indicates the possible existence of identity theft".

What is Identity Theft? It is a fraud committed or attempted using the identifying information of another person without authority. [16 CFR 603.2(a)]. *Identifying Information* is any name, number or biometric data that may be used, alone or in conjunction with any other information, to identify a specific person.

> The creation of a *fictitious identity* using any single piece of information belonging to a real person falls within the definition of ''identity theft'' because such a fraud involves ''using the identifying information of another person without authority.'' [72 Fed.Reg. 63723]

What does this have to do with your municipal client? Several of their operations make municipalities creditors. All creditors must comply with the Red Flag Rule. The Federal Trade Commission (FTC) is the regulatory agency to which they are accountablep0. [See Attachment 1, Final Rule, 72 Fed.Reg 63771 et seq., November 9, 2007.]

I. THE LIABILITY RISKS

A. ENFORCEMENT OF THE RULE

Both the FTC and the state's chief law enforcement officer may bring actions for violations of FACTA. The state's chief law enforcement officer may seek money damages against violators. Only federal or state officials may enforce the Red Flag Rule. 15 U.S.C. §1681m(h)(8).

What constitutes a violation? The Fair Credit Reporting Act (FCRA) seems to equate compliance with performing the duties required by the statute. In the section that was amended by FACTA, it states: "*Compliance*. A person shall not be liable for failure to perform the duties required by this section if, at the time of the failure, the person maintained reasonable policies and procedures to comply with this section." 15 U.S.C. §1681m(h)(7).

If a creditor performs all of the actions required by the Red Flag Rule, has it complied with FACTA even though one or some of its acts were incorrect? Put another way, does a good faith effort defeat an enforcement action?

1. FTC Enforcement powers: In the event of a "knowing violation that constitutes a pattern or practice of violations," the FTC may commence a civil action to recover a civil penalty of up to $2500.00 per violation. [15 U.S.C. § 1681s(a)(2)]

2. State enforcement powers: The chief law enforcement officer of a State or a State-designated agency has the power to bring an action to enjoin a violation if there is reason to believe that a person has violated or is violating the FACT Act. The action may be brought in federal district court or in any other court of competent jurisdiction.

   In addition, the state officer may bring an action on behalf of the residents of a state to recover damages of not more than $1000.00 for each willful or negligent violation, and costs of the action and reasonable attorney fees. [15 U.S.C. § 1681s(c).]

B. ACTIONS IN TORT:

Although a consumer may not bring an action to enforce the Red Flag Rule, does a victim of identity theft have a separate cause of action grounded in traditional tort analysis? A creditor's duty in compliance with the Rule is to develop and implement a written Identity Theft Prevention Program in accordance with defined actions and criteria.

If there were no federal or state statutes and no Red Flag Rule, would a creditor have a legal duty to maintain and protect its records in a manner reasonably designed to prevent, detect and/or mitigate identity theft? A tort analysis suggests that a creditor's duty is broader than the requirements of the Red Flag Rule.

How does the existence of the Red Flag Rule interact with a tort analysis?

a. Even for records that are not covered by the Rule, does the Rule create a new standard of care for prevention of identity theft?

b. If a public body erroneously determines that a transaction is not a covered account subject to the Rule, would any resulting identity theft constitute

negligence per se? Would a victim have an independent cause of action under such circumstances?

c. Would evidence that a specific transaction was managed by the same procedures developed for the creditor's ITPP constitute a defense against allegations of negligence?

C. RISK FROM SUNSHINE LAWS

A "sunshine" or "open records" law creates duties for your municipal client to make most of its records open to the public. Nothing in the Red Flag Rule or FACTA itself requires confidentiality of data, i.e., personal identifying information, in an account. Nothing in these federal mandates absolves your client from complying with state and local requirements pertaining to disclosure of public records.

For example, Oklahoma law states: "All records of public bodies and public officials shall be open to any person for inspection, copying, or mechanical reproduction during regular business hours . . . ." 51 O.S. §24A.5. Although exceptions exist, most municipal records are subject to public disclosure.

Your municipal client's records will include a lot of "personal identifying information": names, addresses, social security numbers, birthdates, government-issued driver's licenses or identification documents, alien registration papers, passport numbers, employer or taxpayer identification numbers, financial information, among other items of data.

How does the Red Flag Rule interact with local Sunshine Laws? Not all data requests will trigger the Red Flag Rule, which only applies to personal identifying information in a "covered account." Therefore, it will be necessary for your client to consider an Open Records Assessment:

a. What records made open to the public under a sunshine law are also data in a "covered account"?
b. What open records requests will constitute a "red flag"?
c. How will your client respond to such a red flag?
d. Does your client really need all the "personal identifying information" it collects?

II. THE FUNDAMENTAL REQUIREMENT

Creditors that offer or maintain a covered account must develop and implement a written Identity Theft Prevention Program to ***detect*, *prevent and mitigate*** identity theft in connection with the opening of a covered account or any existing covered account**.** [16 CFR §681.2(d)(1), 72 Fed.Reg. 63718, 63772]

Who is a creditor?

Creditor: any person who regularly extends, renews, or continues credit. 15 U.S.C. §1681a(r)(5); 16 CFR §681.2(b)(5). This includes collection agencies and other third party debt collectors that have authority to extend, renew or continue credit. 72Fed.Reg. 63722 [discussion of Sections _.90(b)(5) corresponding to FTC §681.2(b)(5).]

Credit: the right granted by a creditor to a debtor to **defer payment**. 15 U.S.C. §1681a(r)(5);16 CFR §681.2(b)(4).

What is a "covered account"?

An account***** designed to permit multiple payments or transactions primarily for personal, family, or household purposes; OR

any other account***** for which there is a reasonably foreseeable risk from identity theft. 16 CFR §681.2(b)(3).

*****_Account_ means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. *Example:* an extension of credit, such as the purchase of property or services involving a deferred payment. 16 CFR §681.2(b)(1).

This includes inactive accounts. 16 CFR §681.2, Supplement A to Appendix A. In response to Section 114 of FACTA, the regulatory agencies identify as a Red Flag specified activity on an inactive account. 72 Fed.Reg. 63733.

STEP 1. DOES YOUR MUNICIPAL CLIENT HAVE COVERED ACCOUNTS?

1. Utility accounts are expressly mentioned in the Rule's definition of covered accounts. They clearly involve an ongoing relationship with a utility customer involving multiple transactions for which payment is deferred until after the service is rendered.

2. Any other recurring service that is offered by your municipal client allowing for deferred payment likely generates a covered account. How does your client collect for ambulance runs, for example?

3. What accounts fall within the category of "any other account for which there is a reasonably foreseeable risk from identity theft"? The FTC and other regulatory agencies issuing the Red Flag Rule specifically rejected the suggestion that the Rule should apply to all transactions. 72 Fed.Reg. 63721.

   Public bodies have numerous records containing personal identifying information, which is the precise data that the Rule is supposed to protect. 72 Fed.Reg. 63723 [discussion of Section_.90(b)(8), corresponding to FTC §681.2(b)(8).] It is easily foreseeable that this information could be as much at risk of identity theft as that contained in a covered account. Therefore, foreseeable risk may not be the only determining factor.

Instead, do we look at the definition of an account? This extends the scope of a covered account to include any ongoing credit relationship, including for business purposes, and presumably may involve only one deferred payment. 72 Fed.Reg. 63721 [discussion of §_.90(b)(3) Covered Account, which corresponds to FTC 16 CFR §681.2(b)(1) and (3).] This becomes important when we consider payment plans for governmental enforcement or regulatory obligations that have no true counterpart in the private, commercial sector.

4. Payment schedules for multiple payments to satisfy court fines, license or permit fees, nuisance abatement payments or other regulatory or enforcement purposes appear to fall within the definition for a "covered account." ***. . .*** *but the FTC is not so sure!*

   a. Deferred Payments: The Dilemma
      i. The payment plan seems to create an ongoing relationship as contemplated by the definition of an account. 16 CFR §681.2(b)(1). Maintenance of such an account could foreseeably create a risk of identity theft.

      ii. This writer was advised <u>informally</u> that the FTC may not enforce the rules against a court payment plan. *[per my telephone conversation with a lawyer for the Federal Trade Commission]*

      iii. This type of governmental activity does not correspond to private sector experience or usual credit transactions. Even so, the agency has recognized that the second prong of the "covered account" definition is designed to be broader than consumer transactions. 72 Fed.Reg. 63721 [discussions for each definition for "account" and "covered account".]

      iv. The issue: whether allowing a person to pay a fine over time with deferred payments is a <u>service</u> as contemplated in the agencies' comments on the scope of the Rule. *Id.*

   b. What is a Service?
      i. Neither the applicable federal rules nor statutes have a definition of "service". When asked what a municipality would cite to a court in an action against the municipality based on identity theft from court payment plans, the FTC lawyer agreed that FACTA and FCRA do not provide such authority.

      ii. Do we look to the underlying transaction or do we look to the payment plan – the account – itself to resolve the issue?

   c. Municipal Court Identity Theft Plan?
      It is not necessary to create a separate ITPP for municipal court if
      - the court's covered activities are included in the overall plan and
      - the appropriate employees in the court clerk's office are trained to administer the Program

d. The same analysis would apply to other deferred payment arrangements for governmental enforcement or regulatory obligations.

e. The Risk of Liability
Assuming that the Rule does not apply to uniquely governmental obligations, does your municipal client risk liability when a judge is confronted with a victim of identity theft from a payment plan maintained to satisfy such obligations?

5. What is NOT a covered account? [some frequently asked questions]
   a. Merely *accepting credit card payment* does not invoke the Red Flag Rule. In such a transaction, the payee is a vendor. The creditor is the credit card issuer.

   b. Court citations do not fall within the Rule even though the ticket is paid at a later time than the date the citation is issued,
      - there are <u>not</u> multiple transactions *and*
      - the imposition of a fine or penalty assessment is <u>not a product or service</u> *and*
      - there is <u>no credit</u> and no ongoing relationship because nothing is owed until the defendant becomes obligated to pay.

   c. Where a contractor, for example, obtains a building permit multiple times during a year and pays for each permit at the time it is issued, the individual transactions do not constitute a covered account because
      - application for separate permits or licenses do not establish one <u>ongoing relationship</u>;
      - there is no account designed to permit multiple transactions; and
      - credit is not extended, i.e., there is <u>no deferred payment</u>.

STEP 2: IS YOUR CLIENT'S RISK ASSESSMENT REASONABLE?

A creditor is told to conduct a risk assessment to determine whether it has covered accounts and to take into consideration (a) the methods it provides to open its accounts, (b) the methods it provides to access its existing accounts, and (c) any previous experiences with identity theft. [16 CFR § 681.2(c), 72 Fed.Reg. 63718, 63772].

This dovetails with the further requirement that the creditor must develop reasonable policies and procedures to identity and detect Red Flags. [16 CFR §681.2(d)(2), 72 Fed.Reg. 63718, 63772].

The results of the risk assessment will lead to an individualized Identity Theft Prevention Program (ITPP). Each creditor's ITPP must be appropriate to its size and complexity and the nature and scope of its activities. [16 CFR § 681.2(d)(1), 72 Fed.Reg. 63718, 63772]. This means that your municipal client must create a program that is *customized* by it for its activities and must be *risk-based*.

A. THE PROBLEM

So, why do so many ITPPs look alike? I have provided a copy of an ITPP adopted by the City of Jenks, Oklahoma. [See Attachment 2.] This program is very similar in both format and content to examples of ordinances retrieved through a Google search from Colorado, Washington, Kentucky, Illinois and a sample from the Georgia Municipal League. These in turn look a lot like private sector examples the Oklahoma Municipal League obtained from credit unions for its September 2008 Red Flag workshop.

The explanation is simple. The Rules tell us that the customized programs must contain standardized elements set out in the Rule itself. [16 CFR §681.2(d)(2)] Furthermore, the final individualized analysis must incorporate specific Guidelines contained in Appendix A to the Rule. [16 CFR §681.2(f)] These elements and Guidelines constitute an outline for an ITPP.

With the development of an ITPP, a creditor has complied with the Rule. Presumably, then, the penalties for noncompliance are not available if an instance of identity theft occurs. Perhaps a case could be made for negligent noncompliance under specific facts and circumstances. But this begs the question. The issue is: where will a victim's lawyer look to make a case for negligence that caused damages to the plaintiff? What lies behind the conclusions that make up the ITPP? THE RISK ASSESSMENT

B. RISK IN THE RISK ASSESSMENT?

The risk assessment is the crux of an ITPP. It is your client's analysis of what it is doing – its practices and procedures -- in order to *identify gaps* in verification and protection of data. Its purpose is to hold up a mirror to the creditor's handling of accounts in order to discover *what* security risks exist and *where* they are.

When notice of the investigation is delivered, the claim is filed or the summons is served, the municipal lawyer may find that the assessment process was cursory and the results were not documented. How then will you establish that the ITPP reasonably addresses the risks of identity theft embedded in your client's methods of opening or handling accounts? What is the evidence that the ITPP reflects the findings of the assessment to allow the detection and/or mitigation of identity theft as it occurs?

IDENTIFYING RED FLAGS

1. HOW COULD A CUSTOMER'S IDENTITY BE STOLEN FROM YOUR CLIENT'S ACCOUNTS?
   - ⇒ Any previous experience(s) with identity theft?
   - ⇒ Lost custody of information?
   - ⇒ Someone intentionally took data?

New Accounts: Verify Information

How could *stolen identity* be used to open a new account?

What identifying information does your client accept: driver's license, I-9 sources, picture ID, passport?

What additional security information does your client require: pet's name, mother's maiden name?

How are remote applications taken and how is identity verified?

Does your client use outside sources for verification assistance?

New Accounts: Application Environment

How could *identity be stolen* while opening a new account?

What is the physical setting where an applicant signs up for service?

What can another customer *see*?

What can another customer *overhear*?

Existing Accounts: Access Controls

How could a *stolen identity* be used to access an existing account?

What process does your client's staff go through to access an existing account?

What controls are in place to limit access by a customer: password, key word/phrase verification, PIN?

Does your client automatically flag address changes?

Existing Accounts: Verify Information

How could *identity be stolen* from an existing account?

What customer identifying information does your client maintain?

Who has access to customer identifying information?

Are there data controls in place for all accounts?

Inactive and Closed Accounts

a. Unusual activity: What triggers attention to new activity in an inactive account?
b. Records retention: Does your client monitor these accounts for risks of identity theft? Who has access to records in off-site storage?
c. Returning Utility Deposits: What data does your client provide with these refunds? Does your client verify the address change – there will almost always be one?
d. Reopen/Reactivate a Closed Account: What verification will your client require for personal identification; for remote requests (e.g., phone, internet); or from third parties?

2. THE RULES INCLUDE A SUPPLEMENT THAT LISTS 26 EXAMPLES OF RED FLAGS.
These examples are guides but *a creditor must include* in its list of red flags all other factors that constitute a risk for your operation.

If you recognize a GAP in your client's current security procedures, identify that gap as a red flag and state in the Program what immediate steps your client will take to deal with the gap as well as its deadline for doing so.

3. RED FLAGS FROM THE GUIDELINES
   This includes taking into consideration:
   - ⇒ Risk Factors
   - ⇒ Sources of Red Flags
   - ⇒ Categories of Red Flags

   [16 CFR Part 681 Appendix A; 72 Fed.Reg. 63773]

DETECTING RED FLAGS

Your client's ITPP must include *its steps* for doing the following:

- ✓ Verifying identity of a person opening an account
- ✓ Authenticating customers' information
- ✓ Monitoring transactions for suspicious activity
- ✓ Verifying validity of address changes

DETECTION TASKS

Customer Information: Verify
Access: Control
Data: Protect
Service Providers: Monitor
Credit Reporting Agencies: Notify

1. Customer Information: Verify
   a. VERIFY New Customers: What forms of identity does your client accept? *Before your client opens an account*, it should have procedures to know that a person is who he/she says they are. This requires extra precautions for online or telephone applications.

   b. VERIFY Existing Customers: Is the person accessing an account actually your client's customer?
      - Flag requests for a change of address. *Address changes are a primary means of identity theft.*
      - Password protect accounts

   c. How does your client process and maintain information for payments
      - Are there different procedures for the various acceptable forms of payment: cash, check, credit card, bank draft, online?
      - If payment is made by telephone, is a credit card or bank routing number repeated aloud so that others can hear it?
      - Is information about online payments secure?
      - Is any information given to third parties who pay a customer's bill?

2. Control Access
   Limit access to only those employees who need to work with the data. Does your client provide staff with passwords for access to computer records?

Are paper records locked in secure storage? What are your client's methods to detect unauthorized access by an employee?

Limit remote access. Restrict information available to field personnel terminals. Establish passwords and security protocols for customers' online transactions.

Manage the environment. Are mirrors behind the computers reflecting the monitor screens? Are computer screens at an angle that allows them to be seen? Are computer monitors for drive-through transactions visible inside the lobby? Is there privacy for talking to customers?

3. Some Data Protection Steps

For computers: Use a firewall. Install an intrusion protection system. Encrypt customer data. What are the procedures for deleting all data and retrieving all disks or software before disposing of a computer?

For records in use: Do not leave any record unattended, including files on a computer. Do computer monitors shut down after a brief period of inactivity?

Purge and shred all old records. Note that FACTA requires any person, including a government agency, who maintains or otherwise possesses sensitive information derived from a consumer report or is derived from a consumer report for a business purpose to properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. 16 CFR §682.3.

4. Monitoring Service Providers

a. Your client is responsible for risks to its accounts even if it outsources an activity to a third-party. [Appendix A to Part 681, IV(c), 72 Fed.Reg. 63773]

A service provider is a third party that your client engages to perform an activity in connection with one or more of its covered accounts. [16 CFR § 681.2(b)(10), 72 Fed.Reg. 63718, 63772]

b. Service Provider Access: This includes any person or entity that is permitted access to customer information in connection with its service to the creditor, such as computer network or maintenance for software, hardware, programmers; collection agencies; records storage

5. Credit Reporting Agencies

IF your client uses consumer reports from a credit agency, its Program must include steps to authenticate that the *report relates to the person about whom it requested the report.* [16 CFR 681.1; 72 Fed.Reg. 63771] There are additional duties to investigate address discrepancies from credit reporting agencies.

III. A CASE STUDY

Red Flag: Creditor. Last September as I was preparing for a workshop on the new Red Flag Rule, I received a letter from my mortgage company. It said, in effect:

> Dear Diane Pedicord,
>
> We are writing to inform you that we recently became aware that one of our employees (now former)
>
> *[ed. That's my favorite part. It alerted me that something <u>not</u> <u>good</u> was about to follow!]*
>
> may have sold personal information about you to a third party. It has been determined that the customer information involved included your name, address, Social Security number, mortgage loan number and *various other loan and application information.*

What would constitute *various other loan and application information*? Well, bank account number, birth date, information about my family, financial information: all this comes to mind.

Response: Creditor. The letter went on to outline the company's cooperation with law enforcement and its intention to monitor my account. They promised to notify me if they detected any suspicious or unauthorized activity. (Note the use of terminology straight from the Guidelines.)

Following the mortgage company's advice, I called one of the credit bureaus and placed a fraud alert on my credit reports and, for reference, obtained a free copy of my report. I took them up on their offer to pay for a two-year membership in a credit monitoring service.

<u>*Consider:*</u> What response should your municipal client take to prevent and/or mitigate identity theft?

Red Flag: Financial Institution. Then, I contacted my bank to protect access to my account. This financial institution, actually a credit union that serves many cities and towns in the state, had supplied one of the private sector examples of an Identity Theft Prevention Program for our September workshop.

I phoned and explained my situation. They asked my name, my address, the last four digits of my Social Security number, and my bank account number. This, of course, is precisely the information that had been sold by the now former employee of the mortgage company. At that point, I could have been anybody!

After being put on hold, I was informed that I could place a password on my account. With much apology, the customer representative told me that I would have to

appear in person with some forms of identification in order to complete this process. I assured her that I was very pleased that this could not be done over the phone.

Response: Financial Institution. The credit union lobby was designed for good customer service. A long bench was situated just inside the door. A couple of steps from the front end of the bench an employee was available at a desk with a computer terminal. This was convenient for folks like me who didn't need to go to a teller window at the far side of the lobby. No one was ahead of me but a gentleman came in and seated himself on the bench as I advanced toward the desk. Armed with my birth certificate and my Social Security card, I explained why I was there.

In that public setting, I was asked to state my name, address, last four digits of my Social Security number, and my bank account number. Then, without requiring any identification, the customer service representative (CSR) asked me to give her my preferred password -- outloud. At that, the gentleman got up and walked to the far end of the bench close to the door and presumably out of hearing range. He was protecting the privacy of my information but the CSR was not.

Consider: That financial institution had gone through a process to identify and detect Red Flags and to develop an Identity Theft Prevention Program. The ITPP, however, does not reveal what was considered in the risk assessment or what was identified as a Red Flag. It does not reveal how the financial institution meant to resolve the tension between good customer service and protection of personal information.

My experience certainly illustrates the necessity for a municipal lawyer to monitor your client's compliance with the Rule's requirement for training staff with responsibilities for covered accounts and with the ongoing review, updating and administration of the Program.

CONCLUSION

The municipal lawyer should assess whether your client the municipal client has complied with the Red Flag Rule. To avoid liability for negligence under any available theory, the municipal lawyer will want to be satisfied that

the client's risk assessment was thorough;
the Identity Theft Prevention Program is complete;
it is being reasonably managed; and
the Program is a living document.