

# **The Red Flag Rule and Beyond: Identity Theft Liability Issues for Municipal Managers**

ICMA Webconference

May 6, 2010

Diane Pedicord  
General Counsel  
Oklahoma Municipal League

Identity theft is more and more a part of everyday life. In fact, it is one of the fastest growing crimes in the world. To counter this trend, the federal government has made possessors of individuals' personal identifying information responsible for containing the risk of identity theft. It's method: the Red Flag Rule.

I submit that the promulgation of this federal rule creates new risks of liability for municipalities extending beyond the Rule's penalties for noncompliance. At the very least, all cities and towns are now on notice of the risks of identity theft. Such notice strengthens negligence theories of liability even in cases not explicitly covered by the Red Flag Rule.

## **WHAT IS THE RED FLAG RULE?**

**REASON FOR THE RULE.** The Red Flag Rule has the purpose of **curtailing identity theft as it occurs**. It implements a series of amendments to the Fair Credit Reporting Act (FCRA), collectively titled the "Fair and Accurate Credit Transactions Act (FACTA)".

**MANDATE OF THE RULE.** Each creditor offering or maintaining a "covered account" must implement and provide for the continued administration of a **written Identity Theft Prevention Program** that identifies red flags to *detect, prevent, 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]

Additional requirements apply to those creditors using credit reporting agencies to reconcile address discrepancies. [16 CFR § 681.1]

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

***What does this have to do with your municipality?*** 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 accountable. [See, 72 Fed.Reg 63771 et seq., November 9, 2007.]

**CAVEAT REGARDING THE RULE.** In evaluating risks, you should note that the Red Flag Rule does not apply to all transactions involving personal information. More importantly, it does not aim to protect data *per se*. It only aims to detect attempted identify theft when it occurs. Therefore, liability risks for identity theft may be broader than intended by the Rule itself.

## **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. [See generally the enforcement sections of FCRA, 15 U.S.C. §1681s.] Only federal or state officials may enforce the Red Flag Rule so there is no civil action available to aggrieved consumers. 15 U.S.C. §1681m(h)(8).

What constitutes a violation? The Fair Credit Reporting Act seems to equate compliance with performing the duties required by the statute. The section that was amended by FACTA 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).

**Query:** 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 \$2,500.00 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 \$1,000.00 for each willful or negligent violation, and costs of the action and reasonable attorney fees. [15 U.S.C. § 1681s(c).]

In my state, the chief law enforcement officer is the Attorney General. This is an elected position and its incumbents often subsequently run for Governor or other

higher office. Under these circumstances, the Attorney General will likely be willing to bring compliance actions, especially in highly-visible cases and/or in an election year.

## **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 contract or tort analysis?

1. The Red Flag Rule only creates a duty for a creditor to develop and implement a written Identity Theft Prevention Program in accordance with defined actions and criteria. The Rule expressly does not cover all credit accounts or all transactions but only those falling within its defined parameters. 72 Fed. Reg. 63720-63721.
2. *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?* Traditional legal analysis suggests that a creditor's duty is broader than the requirements of the Red Flag Rule.

As early as 1961, a bank was held liable to a depositor who suffered damage when the bank disclosed private account information to a third party. Liability was imposed for breach of an implied contract arising from a common law duty of confidentiality. *Peterson v. Idaho First National Bank*, 367 P.2d 284 (Idaho 1961). Subsequent courts, recognizing a common law duty of confidentiality, have applied traditional tort standards. *Patrick v. Union State Bank*, 681 So.2d 1364 (Ala. 1996).

This duty has been extended beyond financial institutions to protect employees whose personal information is not adequately guarded against identity theft. *Bell v. Michigan Council 25 A.F.S.C.M.E.*, 2005 WL 356306 (Mich. App. Feb. 15, 2005), appeal denied, 707 N.W. 2d 597 (Mich. 2005).

Additionally, on December 25, 2009, the Associated Press reported a national mortgage company is seeking to settle a class action emanating from an employee's theft of customers' personal identifying information. The suit alleges the company negligently failed to maintain reasonable procedures to protect customers' sensitive personal information. Theories of liability include common law theories of negligence, bailment, implied contract, invasion of privacy as well as breaches of FCRA and applicable state law. *Elkhettab v. Countrywide Financial Corp, et al*, U.S. District Court for the Central District of California, Case No. CV08-05809

3. Although the preemptions in FCRA apply to FACTA violations, that title specifically contemplates that states may have their own laws and penalties for many instances of identity theft. 15 U.S.C. 1681t(a).
4. How does the existence of the Red Flag Rule interact with a tort analysis?
  - a. Even for circumstances not covered by the Rule, does the Rule create a new standard of care for prevention of identity theft? Does it now establish a basis to determine that harm is foreseeable if a custodian of personal information fails to take reasonable protective measures?
  - b. If a creditor's compliance with its Identity Theft Prevention Plan is not adequate to prevent identity theft, is such compliance a defense that the creditor owes no further duty? On the other hand, may a harmed customer show that his loss was foreseeable even under the ITPP's measures?
  - c. 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?
  - d. Would evidence that a specific transaction not subject to the Red Flag Rule was managed by the same procedures developed for the creditor's Identity Theft Prevention Plan constitute a defense against allegations of negligence?

### **C. The Bottom Line**

In light of the potential for liability under the above-stated unanswered questions, the prudent municipal manager will do more than assure that the municipality has complied with the letter of the Red Flag Rule. Additional risk management factors should be embedded in the risk assessment and review of municipal record creation and management practices.

## **A RED FLAG LIABILITY AUDIT**

A creditor is told to conduct a RISK ASSESSMENT. **This is the crux of an ITPP.** Its purpose is to hold up **a mirror** to your municipality's operations to discover **what** security risks exist and **where** they are.

The Red Flag Rule requires a risk assessment *to determine whether your municipality has covered accounts* and to take into consideration (a) *any previous experiences with identity theft*, (b) *the methods your municipality provides to open its accounts*, and (c) *the methods your municipality provides to access its existing accounts*.

**Risk lurks** (1) if your municipality does not properly identify its covered accounts; (2) from your municipality's duties under other laws; and (3) from the way your municipality conducts its risk assessment!

## STEP 1. DOES YOUR MUNICIPALITY HAVE COVERED ACCOUNTS?

There are **two categories** in the definition of a "covered account" but both involve *deferred payments*.

CATEGORY 1: a consumer account designed to permit multiple payments or transactions primarily for personal, family, or household purposes; such as:

- A. Utility accounts. 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.
- B. Multiple Payments. Any other recurring service that is offered by your municipality allowing for deferred payment likely generates a covered account. How does your municipality collect for ambulance runs, for example?

CATEGORY 2: any other account for which there is a reasonably foreseeable risk from identity theft. *What is this?*

- A. Other Accounts at Risk. What accounts fall within the category of "any other account for which there is a reasonably foreseeable risk from identity theft"? The FTC specifically rejected the suggestion that the Rule should apply to all transactions, so this Category must mean something broader than Category 1 but is nevertheless restricted in its application. Until we receive further guidance from the FTC or the courts, we are left with a bit of guesswork. Following is an attempt to explore the implications for cities and towns.

Foreseeable Risk. Public bodies have numerous records containing personal identifying information, which is the precise data that the Rule is supposed to protect. *It is easily foreseeable that this information could be as much at risk of identity theft as that contained in any covered account.* Therefore, foreseeable risk may not be the only determining factor.

What is an Account? Instead, do we look at the broader definition of an account?

*Account* means a continuing relationship established by a person with a 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.

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*.

Does this include payment plans for governmental enforcement or regulatory obligations that have no true counterpart in the private, commercial sector, e.g. court fines, license or permit fees, nuisance abatement payments? The FTC doesn't think so but a court trying a case of identity theft from precisely that type of governmental record has yet to answer the question.

#### **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 in full at a later time than the date the citation is issued,
  - *there are not multiple transactions and*
  - *the imposition of a fine or penalty assessment is not a product or service and*
  - *there is no credit 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 ongoing relationship;*
  - *there is no account designed to permit multiple transactions; and*
  - *credit is not extended, i.e., there is no deferred payment.*

### **STEP 2: LIABILITY RISKS FOR PUBLIC BODIES**

This paper has already discussed two sources of potential liability for your municipality stemming from the promulgation of the Red Flag Rule: (1) administrative enforcement authority for violation of the Rule itself and (2) the Rule's creation of a new standard of care under a tort liability analysis. Additional risks may arise under state laws promoting accountability by public bodies to their citizens.

#### **A. RISK FROM SUNSHINE LAWS**

A "sunshine" or "open records" law creates duties for your municipality 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 municipality 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 and copying.

Your municipality’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.

- Social Security Numbers may be open.
- Financial Records may be open.

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 municipality 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 municipality respond to such a red flag?
- d. Does your municipality really need all the “personal identifying information” – especially social security numbers -- it collects?

**B. RISK FROM RECORDS RETENTION LAWS**

A state or local law may require your municipality to maintain its records for a designated period of years. Records management and storage mandates may increase risks for identity theft because it could be harder to dispose of personal identifying information. Additionally, even when records are stored offsite or in electronic formats, they may be exposed to access by many more people.

Under the Red Flag Rule, a creditor is responsible for its records even when an account is inactive, closed or managed by a third party. At the same time, nothing in the Rule requires a creditor to destroy or delete personal identifying information. Therefore, a public body must comply with the state records retention mandates and remain subject to monitoring the records for red flags.

**C. OTHER CONSIDERATIONS**

As can be seen from the discussion above, the Red Flag Rule makes no special allowance for the public nature of governmental business. Therefore, the Rule does not

address disclosure issues faced by public bodies for data that private sector businesses may keep as proprietary or confidential. FCRA expressly states that it does not exempt any person subject to its provisions from complying with nonconflicting state laws. 15 U.S.C. §1681t(a). The only option for your municipality is to identify red flags that occur as a result of compliance with state accountability laws.

### **STEP 3: IS YOUR MUNICIPALITY'S RISK ASSESSMENT REASONABLE?**

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. The FTC has been very adamant that the program must be *customized* by each creditor for its activities. The ITPP must be *based on the risks your municipality identifies from its operations*.

#### **A. THE PROBLEM**

So, why do so many ITPPs look alike? On OML's website you can see a copy of an ITPP adopted by the City of Jenks, Oklahoma. 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. Furthermore, the final individualized analysis must incorporate specific Guidelines contained in Appendix A to the Rule. These elements and Guidelines constitute an outline for an ITPP. [See Attachment 1 to this paper.]

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 your municipality's analysis of what it is actually doing – its practices and procedures -- in order to *identify gaps* in verification and protection of data.

When notice of the investigation is delivered, the claim is filed or the summons is served, you 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 municipality'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? *How was the assessment performed? By whom? What did they look at? Was the process documented?*

**THE KEY TO IMPLEMENTING AN ITPP: THE RISK ASSESSMENT**

**This is an analysis of what your municipality is doing now in order to identify gaps in verification and security of data.**

**THE KEY TO AVOIDING IDENTITY THEFT: VERIFICATION**

- ❖ **that persons are who they say they are**
- ❖ **that persons accessing an account have authority to do so**

**A CASE STUDY**

**RED FLAG: CREDITOR.** In September 2008, 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 not good 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.

**Consider:** What response should your municipality 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!

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 you to monitor your municipality's compliance with the Rule's requirement for training staff and with the ongoing review, updating and administration of the Program.

## **CASE STUDY LESSONS**

The Creditor had an ITPP but . . .

How good was its risk assessment?

Did it identify all Red Flags?

Was the staff trained adequately?

Had it been amended to reflect actual experience?

## **CONCLUSION**

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

- The municipality's risk assessment was thorough;
- the Identity Theft Prevention Program is complete;
- it is being reasonably managed;
- staff is properly trained; and
- the Program is a living document

## **Attachment: Using the Guidelines**

**An OUTLINE for Your Municipality's ITPP:** The Basic Elements for a Program as explained in the Guidelines – Supplement A – will serve as the outline for the Identity Theft Prevention Program. These **Guidelines** were mandated by Congress to assist creditors in formulating and maintaining an Identity Theft Prevention Program.

The Guidelines contain the following *elements*.

### Risk Assessment

1. Identify relevant Red Flags for covered accounts and incorporate them into the Program
2. Detect Red Flags that have been incorporated into the Program  
26 Examples of Red Flags listed in a Supplement to the Rule.

The examples are guides but *your municipality must include* in its list of red flags all other factors that constitute a risk for your operation.

### Customer Protection

3. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft

### Managing the ITPP

4. Update: Ensure the Program is reviewed regularly and revised periodically to reflect changes in risks to customers and/or your municipality.
5. Provide for continuing administration of the Program.

## **ELEMENT 1: IDENTIFYING RED FLAGS**

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

- B. HOW COULD *STOLEN IDENTITY* BE USED TO OPEN A NEW ACCOUNT?
- What identifying information does your municipality accept?
- driver's license \* I-9 sources \* picture ID \* passport
  - additional personal information: pet's name, maiden name
- Outside sources for verification assistance

### New Accounts: Verify Information

*Before your municipality opens an account*, it should have procedures to know that persons are who they say they are.

This requires extra precautions for remote applications.

- C. HOW COULD *IDENTITY BE STOLEN* WHILE OPENING A NEW ACCOUNT?

### New Accounts: Application Environment

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

⇒ What can another customer see?

⇒ What can another customer *overhear*?

D. HOW COULD A *STOLEN IDENTITY* BE USED TO ACCESS AN EXISTING ACCOUNT?

Existing Accounts: Access Controls

What process does your municipality'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

⇒ Existing Accounts: Data Controls

VERIFY: Is the person accessing your municipality's account the actual customer?

- Flag requests for a change of address. *Address changes are a primary tool of identity theft.*
- Password protect accounts

What identity verification for payments

- by telephone or internet or credit cards of third parties?
- Acceptable Forms of Payment?  
Cash \* Check \* Credit Card \* Bank Draft \* Online

E. HOW COULD *IDENTITY BE STOLEN* FROM AN EXISTING ACCOUNT?

Existing Accounts: Verify Information

How does your municipality maintain customer identifying information?

⇒ Paper records

⇒ Computer records

Who has access to customer identifying information?

Control Access

a. Limit access: only those employees who work with the data

What are your municipality's methods to detect an employee's unauthorized access?

b. 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?

c. Remote access: field personnel terminals?

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, which maintains or otherwise possesses sensitive information derived from a *consumer report* 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.

#### F. INACTIVE AND CLOSED ACCOUNTS: VERIFY IDENTITY

⇒ Records retention: Does your municipality monitor these accounts for risks of identity theft? Who has access to records in off-site storage?

⇒ Returning Utility Deposits? What verification will your municipality require

- for personal identification
- for the address change – there will almost always be one.

⇒ Reopen/Reactivate Closed Account: What verification will your municipality require

- for personal identification
- for remote requests (e.g., phone, internet)
- from third parties

### **ELEMENT 2: DETECT RED FLAGS**

#### **A. WHAT ARE YOUR MUNICIPALITY'S STEPS FOR:**

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

#### **B. SUSPICIOUS ACTIVITY**

⇒ Suspicious Information:

- Documents provided for identification appear to be altered.
- Personal information inconsistent with external information sources

⇒ Unusual use of account:

Account used in a manner that is not consistent with historical patterns of activity

⇒ Data Security Incident: unauthorized access

C. NOTICE OF SUSPICIOUS ACTIVITY

- ⇒ Customer notice of unauthorized charges
- ⇒ Customer notice that it provided information to a fraudulent third party
- ⇒ Fraud or other alerts from consumer reporting agencies
- ⇒ Returned mail despite billable transactions

D. SERVICE PROVIDERS

Your municipality is responsible for risks to its accounts even if it outsources an activity to a third-party.

A service provider is a third party that a creditor engages to perform an activity in connection with one or more of its covered accounts.

⇒ Service Provider Access

This includes any person or entity that is permitted access to customer information in connection with its service to the creditor.

- Computer network or maintenance –
  - Software, Hardware installation Programmers
- Collection agencies
- Records Storage

⇒ Monitor Service Providers

If your municipality uses a service provider for its accounts, it will need to insure that the provider is protecting against identity theft in connection with this activity.

One option is to include red flag requirements in any service contract and assign penalties and risk of loss to the provider if the contract procedures are not followed. Include requirements that the service provider will promptly report to your municipality any red flags connected to your municipality's accounts.

E. CREDIT REPORTING AGENCIES

IF your municipality uses consumer reports from a credit agency, its ITPP must include its steps to authenticate that the *report relates to the person about whom it requested the report*.

**ELEMENT 3: RESPOND TO RED FLAGS: PREVENT AND/OR MITIGATE**

A. Your municipality's response plan must be part of its adopted program.

Your municipality's appropriate response will depend on its particular circumstances, including the risk associated with the Red Flag. This must be customized to your municipality's operations and activities.

B. The Response Purpose: TO CURB IDENTITY THEFT AS IT OCCURS.

C. Relationship with Law Enforcement? Has your municipality arranged for prompt and serious response to reported identity theft?

#### D. Appropriate Responses to Red Flags

- ⇒ Monitor accounts for evidence of identity theft
- ⇒ Contact customer
- ⇒ Change passwords, security codes or other security devices
- ⇒ Close and reopen account
- ⇒ Refuse to open account
- ⇒ Don't collect on or sell account
- ⇒ Notify law enforcement
- ⇒ Determine and document that no response is needed

#### **ELEMENT 4: UPDATING YOUR PROGRAM**

Your municipality's Program must be a living document.

- ⇒ Your municipality must **review** and **modify** it periodically to reflect changes in risks and actual experience with the workings of its ITPP.
- ⇒ Who is responsible for this task?

#### **ELEMENT 5: ADMINISTERING THE PROGRAM: Carrying out the Required Steps**

- ⇒ **RESPONSIBILITY:** Who will manage the day-to-day application of the Program?
- ⇒ **OVERSIGHT:** Who will ensure that the Program is in compliance with the FACT Act?
- ⇒ **TRAINING** staff to implement the ITPP: What is the training schedule? What is the training format? Who is responsible for the training?

### TIMELINE: Effective Date = June 1, 2010

#### Timeline – *Before June 1*

- Complete a Risk Assessment
- Identify Red Flag events that could occur
- Revise or develop policies to establish an Identity Theft Prevention Program (ITPP)
- Write the ITPP

#### Timeline – *By June 1*

- Governing body approves the ITPP
- Appoints Compliance Administrator
- Train Key Personnel
- Implement the Program

#### Timeline – *After June 1*

- Operate the Program
- Conduct a mid-year review – (optional)
- Conduct an end-of-year review – *June 1*
- Prepare and submit a written report to the Governing Body/Oversight Committee