

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

Diane Pedicord  
General Counsel  
Oklahoma Municipal League

October 2009

Identity theft is more and more a part of everyday life. How many of us have received a notice telling us that the account for our bank debit card or a credit card is being closed because our account information has fallen into the hands of an “unauthorized person”? Although fraud is not new, this method of fraud – IDENTITY THEFT – is one of the fastest growing crimes in the world.

To counter this trend, Congress is holding YOU responsible for containing the risk of identity theft. It’s method: the Red Flag Rule.

## OVERVIEW OF THE RED FLAG RULE

**MANDATE OF THE RULE.** Each creditor offering or maintaining a “covered account” must implement 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]

**REASON FOR THE RULE.** The Red Flag Rule has the purpose of **curtailing identity theft**. It stems from congressional legislation and is promulgated by the Federal Trade Commission (FTC) to comply with the Fair and Accurate Credit Transactions Act of 2003 (FACTA or FACT Act).

### **FOCUS OF THE RULE**

- the opening of a covered account,
- accessing any existing covered account [16 CFR § 681.2(d)(1), 72 Fed.Reg. 63718, 63772]
- address discrepancies

**SCOPE OF THE RULE.** The Rule applies to any entity, including a public entity, that establishes “covered accounts” –

- involving **multiple transactions**
- for which **payment is deferred** until after the service is rendered

OR any other account for which there is a reasonably foreseeable risk from identity theft.

This includes inactive accounts and maintenance of inactive account information.

**METHODOLOGY OF THE RULE.** Conduct a **RISK ASSESSMENT** to identify red flags. These are security gaps in protecting customer personal information or in detecting identity theft.

## **UNDERSTANDING THE RED FLAG RULE**

### **TERMINOLOGY OF THE RULE.**

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

**B. What is Identity Theft?** It is a fraud committed or attempted using the identifying information of another person without authority. [See, 16 CFR 603.2(a)]

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]

**Identifying Information:** any name, number or biometric data that may be used, alone or in conjunction with any other information, to identify a specific person.

**C. What does this have to do with you?** Several of your operations make you a *creditor*. All creditors must comply with the Red Flag Rule.

**D. Who is a creditor?**

Creditor: any person who regularly extends, renews, or continues credit. This includes *collection agencies and other third party* debt collectors that have authority to extend, renew or continue credit.

Credit: the right granted by a creditor to a debtor to **defer payment**.

### E. 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.

\**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. *This includes inactive accounts.*

## BASIC ELEMENTS OF A PROGRAM

**An Individualized Program:** Your ITPP must be *customized* by you for your activity and must be *risk-based*. Your Program should be tailored to the size, complexity and nature of your operations.

[16 CFR 681.2(d)(1); 72 Fed.Reg. 63718, 63772]

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

A. 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

#### Customer Protection

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

#### Managing the ITPP

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

B. RED FLAGS from the SUPPLEMENT to the GUIDELINES applicable to municipal operations (Element 1)

- A consumer fraud or active duty alert
- Any account that would adversely affect a consumers credit standing should be considered at risk of identity theft

- A company's knowledge of a security breach within it's own confines or that of an affiliate with which the company has shared data
- Suspicious actions by employees with sensitive customer account information
- An address discrepancy reported by a consumer reporting agency
- A customer's communications about attempted or actual identity theft
- Attempts to open new accounts with altered documents

C. To IDENTIFY RED FLAGS (Element 1), you must consider the following factors:

- ⇒ Risk Factors
- ⇒ Sources of Red Flags
- ⇒ Categories of Red Flags

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

1. Risk Factors:

- The number of accounts served by a utility
- The methods available to open new accounts or to open additional accounts billed to existing customers
- The methods available to complete transactions
- The methods available to view and change information such as customer name, billing address, service address, or auto pay settings

2. Sources of Red Flags:

- Incidents of identity theft the creditor has experienced
- Methods of identity theft the creditor has identified that reflect changes in identity theft risk
- Any existing policies designed to spot risks

3. Categories of Red Flags:

- Alerts from consumer agencies = Fraud or active duty alert included in reporting consumer report
- Suspicious documents = Documents provided for identification appear to be altered.
- Suspicious 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
- Notice from customers = Customer notifies you of unauthorized charges

D. To DETECT RED FLAGS (Element 2), your Program must include *your 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

E. RESPOND TO RED FLAGS: prevent and/or mitigate (ELEMENT 3)

1. Aggravating Factors: What may heighten risks of identity theft?

- a data security incident that results in unauthorized access to a customer's account records
- notice from a customer that information related to your account to someone fraudulently claiming to represent you or to a fraudulent website.

2. Appropriate Responses to Red Flags are set out in the Guidelines.

Response

- 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

F. UPDATING YOUR PROGRAM (Element 4): Factors you must consider:

- Experience with identity theft
- Changes in methods of identity theft
- Changes in methods to detect, prevent and mitigate identity theft
- Changes in types of accounts offered
- Changes in business arrangements

G. ADMINISTERING YOUR PROGRAM (Element 5)

1. Required steps in administering the Program

- Obtain approval of the written Program by your Governing Body or an appropriate authority designated by it.
- Ensure oversight by the Governing Body, or a designated senior manager, of the development, implementation, and administration of the Program
- Train staff, as necessary, to effectively implement the Program
- Exercise appropriate and effective oversight of service provider arrangements

2. Oversight Includes

- Assigning specific responsibility

- Reviewing reports
- Approving material changes in the Program
- Monitoring service providers

Report Requirements:

- At least annually
- Address material matters
  - ✓ Service provider arrangements
  - ✓ Effectiveness of the policies and procedures in addressing the risk of identity theft in connection with covered accounts
  - ✓ Significant incidents involving identity theft and management's response
- Recommendations for material changes to the Program

3. Training Staff

All employees who work with your covered accounts must be trained to

- Identify Red Flags
- Report and React appropriately to Red Flags
- Handle personal information in your accounts

4. Service Provider

This is a person that provides a service directly to the creditor, including any person or entity that maintains, processes, or otherwise is *permitted access to customer information* in connection with its service to the creditor. [16 CFR § 681.2(b)(10), 72 Fed.Reg. 63718, 63772]

H. CREDIT REPORTING AGENCIES

1. Additional RULES for Users of Credit Reports

These apply when a creditor receives a notice of address discrepancy.  
[16 CFR 681.1; 72 Fed.Reg. 63771]

Notice of Address Discrepancy: a notice sent to the user by a consumer reporting agency that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the credit reporting agency's file for the consumer.

- You must have procedures to enable you as user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report when such notice is received.
- Your Program should include procedures for using the information about the address discrepancy.

2. Additional DUTIES for Users of Credit Reports

Develop methods for forming a reasonable belief about a consumer's identity:

- Compare the information in the consumer report with other information you have obtained and/or
- Verify the information in the consumer report directly with the consumer
- If you regularly provide information to a credit agency, you must furnish your verified address for a consumer with whom you have established a continuing relationship.

## **A RED FLAG AUDIT**

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

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

This dovetails with the further requirement that the creditor must develop reasonable policies and procedures to identify and detect Red Flags. Risk lurks (1) if you do not properly identify your covered accounts; (2) from your duties under other laws; and (3) from the way you conduct your risk assessment!

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

Recall that there are **two prongs** to the definition of a "covered account."

PRONG 1: an account\* designed to permit multiple payments or transactions primarily for personal, family, or household purposes; **OR**

PRONG 2: any other account\* for which there is a reasonably foreseeable risk from identity theft.

\**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.

- A. Utility accounts = Prong 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.

- B. MULTIPLE PAYMENTS = PRONG 1. Any other recurring service that is offered by your municipality allowing for deferred payment likely generates a covered account. How do you collect for ambulance runs, for example?
- C. OTHER ACCOUNTS AT RISK = PRONG 2. 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 Prong must mean something broader than Prong 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? 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.* This becomes important when we consider payment plans for governmental enforcement or regulatory obligations that have no true counterpart in the private, commercial sector.

- D. 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!*
1. Deferred Payments: The Dilemma
    - a. The payment plan seems to create an ongoing relationship as contemplated by the definition of an account. Maintenance of such an account could foreseeably create a risk of identity theft.
    - b. This writer was advised informally 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]*
    - c. 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.

- d. The issue: whether allowing a person to pay a fine over time with deferred payments is a service as contemplated in the agencies' comments on the scope of the Rule.
2. 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 Fair Credit Reporting Act of which it is a part 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?
  3. 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
  4. The same analysis would apply to other deferred payment arrangements for governmental enforcement or regulatory obligations.
  5. The Risk of Liability

Assuming that the Rule does not apply to uniquely governmental obligations, does your municipality risk liability when a judge is confronted with a victim of identity theft from a payment plan maintained to satisfy such obligations?
- E. 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: THE LIABILITY RISKS

### 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 you 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. It appears that Texas law is just as broad.

*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.

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 you 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 you respond to such a red flag?
- d. Does your municipality really need all the “personal identifying information” it collects, especially Social Security numbers?

### B. 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). Even so, the Attorney General is elected and will likely be willing to bring compliance actions, especially in highly-visible cases.

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).

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).]

### C. 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 a traditional negligence analysis? A creditor’s duty under 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.

Even for records not subject to the Red Flag Rule, does the Rule establish a new standard of care for tort purposes? When you go through the risk assessment process mandated by the Rule, are you thereby on notice of risks? If those risks aren’t adequately (reasonably?) addressed and an incident of identity theft occurs, is that negligence?

### STEP 3: IS YOUR 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 your program must be *customized* by you for your activities. It must be *based on the risks you identify from your 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.

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 analysis of what you are actually doing – your 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 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?*

## USING THE GUIDELINES FOR YOUR ASSESSMENT

Your Program is required to *include the Guidelines* that are appropriate to your operation. The Guidelines contain the following elements.

### ELEMENT 1: IDENTIFYING RED FLAGS

#### A. HOW COULD A CUSTOMER'S IDENTITY BE STOLEN FROM YOUR OPERATIONS?

- ⇒ Any previous experience(s) with identity theft?
- ⇒ Lost custody of information?
- ⇒ Someone intentionally take data?

#### New Accounts: Verify Information

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

What identifying information do you accept?

- driver's license \* I-9 sources \* picture ID \* passport
- additional personal information: pet's name, maiden name

Remote Applications: how to verify identity?

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 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

#### Existing Accounts: Verify Information

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

What customer identifying information do you maintain?

- ⇒ Paper records
- ⇒ Computer records

Who has access to customer identifying information?

#### Inactive and Closed Accounts: Verify Identity

- Records retention: Do you monitor these accounts for risks of identity theft?
  - Who has access to records in off-site storage?
- Returning Utility Deposits? What verification will you require
  - for personal identification

- for the address change – there will almost always be one.
- Reopen/Reactivate Closed Account: What verification will you require
  - for personal identification
  - for remote requests (e.g., phone, internet)
  - from third parties

**B. THE RULES INCLUDE A SUPPLEMENT THAT LISTS 26 EXAMPLES OF RED FLAGS.**

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

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

**ELEMENT 2: DETECT RED FLAGS**

**A. 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 do you accept?  
*Before you open an account, have procedures to know that a person is who he/she says they are. This requires extra precautions for online applications.*
  - b. VERIFY Existing Customer: Is the person accessing your account your customer?
    - Flag requests for a change of address. *Address changes are a primary tool of identity theft.*
    - Password protect accounts
  - c. 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
2. Control Access
  - a. Limit access: only those employees who work with the data
  - b. Manage the environment:
    - mirrors behind the computers?
    - angles of the computers?
    - privacy for talking to customers?
  - c. Remote access: field personnel terminals?

3. Data Protection Steps
  - Use a firewall
  - Install an intrusion protection system
  - Encrypt customer data
  - Purge and shred old records
4. Monitoring Service Provider Access
  - This includes any person or entity that is permitted access to customer information in connection with its service to You, the creditor.
    - Computer network or maintenance - Software, Hardware installation
    - Programmers
    - Collection agencies
    - Records Storage
5. Credit Reporting Agencies
  - IF you use consumer reports from a credit agency, your Program must include your steps to authenticate that the *report relates to the person about whom you requested the report.*

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

- A Your response plan must be part of your adopted program.  
Your appropriate response will depend on your particular circumstances, including the risk associated with the Red Flag. This must be customized to your operations and activities.
- B. The Response Purpose: TO CURB IDENTITY THEFT AS IT OCCURS.

**ELEMENT 4: UPDATING YOUR PROGRAM**

- Your Program must be a living document.  
You must **review** and **modify** it periodically to reflect changes in risks and your experience with the workings of your Program.

**ELEMENT 5: ADMINISTERING YOUR PROGRAM: Carrying out the Required Steps**

Step 1: Approval by the Governing Body

Completing the Risk Assessment and Writing the Plan

- Who should conduct the assessment?
- Who should review the assessment?
- Who should be involved with the development of the Program?

Steps 2: Oversight Responsibility

Who will ensure that the Program is in compliance with the FACT Act?  
Governing Body? Oversight Committee? Senior Administrator?

Who will manage the day-to-day application of the Program?

### Step 3: Training Staff

This purpose is to implement your ITPP to *identify and to respond* to red flags as they occur.

Response includes knowing how to report red flags. What is the chain of responsibility?

You do not have to train all employees who might have access to your data; *however* all employees who have access to your data should understand your duties to prevent identity theft.

You may consider a code of conduct for such employees for safeguarding your data.

### Step 4: Monitor Service Providers

If you use a service provider for your accounts, you 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 you any red flags connected to your accounts.

You are ultimately responsible for complying with the final rules and guidelines even if you outsource an activity to a third-party.

## **TIMELINE**

### **Timeline – Before November 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 November 1**

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

### **Timeline – After November 1**

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

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

This is an analysis of what you are 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.** 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 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!

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 you to monitor your 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.

## **CASE STUDY LESSONS**

The Creditor had an ITPP but . . .

How good was its risk assessment?

Did it identify all Red Flags?

Issues: staff training; updating the ITPP

## **CONCLUSION**

Each municipality should assess whether you have complied with the Red Flag Rule. To avoid liability for negligence under any available theory, you will want to be satisfied that

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

### **THREE PRINCIPAL ELEMENTS FOR CURBING IDENTITY THEFT**

1. Identify Risks
2. Develop Identification Methods
3. VERIFY    VERIFY    VERIFY