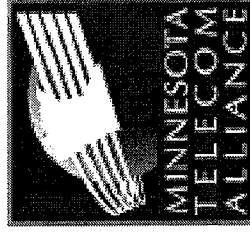


---

**FTC RED FLAG RULES**  
***Implementing the Fair and Accurate  
Credit Transactions Act with an  
Identity Theft Prevention Program***

**September 26, 2008**

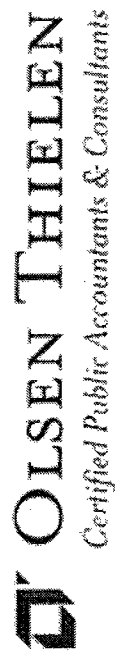
**MTA Managers Conference  
St. Cloud, MN**



---

**FTC Red Flag Rules**  
**Implementing the Fair and Accurate Credit Transactions Act with an**  
**Identity Theft Prevention Program**

Presented by:  
Cecilia Ray – Moss & Barnett  
and Patrick Holton – Olsen Thielen



# **Outline of Presentation**

---

- Background
- Risk Assessment – creditor with covered accounts
- Identity Theft Prevention Program
  - Requirements/Elements
  - Red Flag Rules vs. CPNI Rules
  - Red Flags
    - Detecting
    - Responding (prevent and mitigate)
  - Updating Program
  - Administering Program
  - Enforcement of Rules

# **Statutory Provisions Implemented**

---

- Fair and Accurate Credit Transactions Act of 2003 (FACT Act) amends the Fair Credit Reporting Act (FCRA)
- New regulations implement Section 114 of the FACT Act
  - Procedures for identification of possible instances of identity theft (Identity Theft Prevention Program)

# **Background**

---

- Regulations result from joint rulemaking:
  - FTC, Dept. of Treasury (Offices of Comptroller and Thrift Supervision, Federal Reserve, FDIC, Nat'l Credit Union Admin.
- Final rules published November 9, 2007
- **Full compliance required by November 1, 2008**
  - Program adopted by Board and employees trained

# **Identity Theft Red Flags**

---

- FACT Act Section 114
- Amends Fair Credit Reporting Act Section 615(e) (15 USC Section 1681m)
- Agency Regulations: 12 CFR 41.90
- Risk-based final rules – flexibility for creditor to develop Program appropriate for it
- Guidelines provided in Regulations
- Supplement A to Appendix J - 26 examples of Red Flags

## **Step One: Risk Assessment**

- Each financial institution and **creditor** to *periodically* determine whether it offers or has **covered accounts**.
- Consider:
  - Types of accounts offered or maintained
  - Methods to open accounts
  - Methods to access accounts
  - Previous experience with identity theft

# **Definitions**

---

## **A "creditor":**

- Regularly extends, renews or continues credit
- Regularly arranges for the extension, renewal or continuation of credit, or
- Any assignee of an original creditor who participates in the decision to extend, renew or continue credit
- Includes utility companies and telecommunications companies

# **Definitions (cont'd)**

---

## **A "covered account" is:**

- An account offered or maintained primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions
- Credit card, mortgage or car loan, cell phone, utility account

**OR**

- Any other account for which there is a reasonably foreseeable risk of identity theft

# **Program Requirement**

Financial institutions and creditors with covered accounts must 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*

# **Program Requirement**

**(cont'd)**

---

- If required to implement a Program, must consider the Guidelines in Appendix J of the Regulations, and include those appropriate

# Program Requirement

## (cont'd)

---

- Identity Theft Prevention Program must be appropriate to:
  - the size and complexity of the financial institution or creditorand
  - the nature and scope of its activities.
- Program may incorporate, as appropriate, existing policies and procedures that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor
  - CPNI compliance program useful, but not complete for Identity Theft Prevention Program

# Red Flag Rules vs. CPNI Rules

- CPNI: protect telecommunications customers from pretexting and unauthorized use or disclosure of personally identifiable customer information
  - Using identity of another to gain access to call detail or other personally identifiable information
- Red Flags: protect all customers (and creditors) with covered accounts from identity theft
  - Fraud attempted or committed using identifying information of another without authority

# **Elements of the Program**

## **Must include policies and procedures to:**

- *Identify relevant Red Flags and incorporate them into the Program*
- *Detect Red Flags that are part of the Program*
- *Respond appropriately to any Red Flags that are detected*
  - Prevent and mitigate
- *Ensure the Program is updated periodically to address changing risks*

# Elements of the Program (cont'd)

---

Program to include:

- ID Red Flags relevant to your company
- ID action/procedures to detect Red Flags
- ID action/procedures to prevent and mitigate Red Flags
- Designate who's responsible for oversight, implementation and administration (annual review)
- Describe employee training
  - Written acknowledgement by employees of training

# **Red Flags**

- **A Red Flag** is a “pattern, practice, or specific activity that indicates the possible existence of identity theft.”
  - Regulations (Appendix J) identify five categories of Red Flags, with twenty-six examples

## **Identifying Relevant Red Flags**

- Consider information from Risk Assessment
- Include relevant Red Flags from Regulations

# **Identifying Relevant Red Flags**

## **(cont'd)**

---

- **Five Categories:**
  - Alerts, notifications, or other warnings from consumer reporting agencies or service providers, including fraud detection services
  - Suspicious documents
  - Suspicious personal identifying information, including suspicious address change
  - Unusual use of, or other suspicious activity related to, a covered account
  - Notice from customers, victims of identity theft or others regarding possible identity theft in connection with a covered account

## **Alerts, notifications, or other warnings from consumer reporting agencies or service providers, including fraud detection services**

---

1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy, as defined in 12 CFR §41.82(b).
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
  - a. A recent and significant increase in the volume of inquiries;

**Alerts, notifications, or other warnings from consumer reporting agencies or service providers, including fraud detection services (cont'd)**

---

- b. An unusual number of recently established credit relationships;
- c. A material change in the use of credit, especially with respect to recently established credit relationships; or
- d. An account that was closed for cause of identified for abuse of account privileges by a financial institution or creditor.

## **Suspicious Documents**

---

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting identification.

## **Suspicious Documents (cont'd)**

---

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

# **Suspicious Personal Identifying Information**

---

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

- a. The address does not match any address in the consumer report; or
- b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

# **Suspicious Personal Identifying Information (cont'd)**

---

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

# **Suspicious Personal Identifying Information (cont'd)**

---

- a. The address on an application is the same as the address provided on a fraudulent application; or
- b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

# **Suspicious Personal Identifying Information (cont'd)**

---

- a. The address on an application is fictitious, a mail drop, or a prison; or
- b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

## **Suspicious Personal Identifying Information (cont'd)**

---

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

## **Suspicious Personal Identifying Information (cont'd)**

---

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

## **Unusual Use of, or Suspicious Activity Related to, the Covered Account**

---

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

## **Unusual Use of, or Suspicious Activity Related to, the Covered Account (cont'd)**

---

- a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
- b. The customer fails to make the first payment or makes an initial payment but no subsequent payments

# **Unusual Use of, or Suspicious Activity Related to, the Covered Account (cont'd)**

---

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
- a. Nonpayment when there is no history of late or missed payments;
  - b. A material increase in the use of available credit;
  - c. A material change in purchasing or spending patterns;
  - d. A material change in electronic fund transfer patterns in connection with a deposit account; or
  - e. A material change in telephone call patterns in connection with a cellular phone account.

## **Unusual Use of, or Suspicious Activity Related to, the Covered Account (cont'd)**

---

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

## **Unusual Use of, or Suspicious Activity Related to, the Covered Account (cont'd)**

---

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

**Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor**

---

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

## **Detecting Red Flags**

- Verify identity of person opening a covered account
- Authenticate customers
- Monitor transactions
- Verify validity of address changes

# Responding Appropriately to Red Flags

---

- Respond commensurate with degree of risk posed by detected Red Flag and consider aggravating factors that may heighten risk of identity theft
  - Monitor accounts
  - Contact customer
  - Change passwords
  - Close and reopen account with new account number
  - Refuse to open new account
  - Don't collect on or sell account
  - Notify law enforcement
  - No response

# **Periodic Updating of the Program**

- Periodic updating required to reflect changes in risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on:
  - 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

# **Administering the Program**

---

- Initial approval by Board of Directors or appropriate committee of Board
- Involve the Board, an appropriate committee of Board, or designated senior management employee in oversight, 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

## **Administering the Program (cont'd)**

- **Oversight by Board of Directors, committee of same, or designated senior management employee:**
  - Assign specific responsibility for implementing Program
  - Reviewing staff reports on compliance
  - Approving material changes to the Program

# Administering the Program (cont'd)

---

## Report Requirements:

- Report on compliance at least annually to Board, its committee or senior management designee
- Address material matters and evaluate
  - Effectiveness of the policies and procedures in addressing the risk of identity theft in connection with covered accounts
  - Service provider arrangements
  - Significant incidents involving identity theft and management's response
  - Recommendations for material changes to the Program

# **Administering the Program**

## **(cont'd)**

---

### **Oversight of service providers arrangements**

- If engage a service provider to perform activities in connection with a covered account, must ensure the service provider's activities are conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft
- Require service provider to have a Program, and report Red Flags to creditor or take appropriate steps to prevent or mitigate identity theft

# **Administering the Program**

**(cont'd)**

---

- Train employees who interact with customers and billing records, credit records and credit reporting
  - Provide training and a copy of the Program – existing and new employees
  - Both supervisory and staff personnel
- Refresher training annually

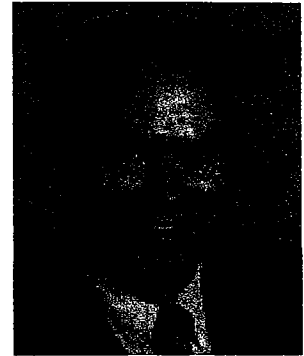
# **Enforcement of Red Flag Rules**

---

- Administrative enforcement under 12 USC 1818
- Private right of action for negligent non-compliance?
- State Attorneys General
- No criminal penalties

## **Patrick D. Holton Telecommunications Consultant**

Pat is a Manager and Senior Telecommunications Consultant in the Consulting Department of the St. Paul office of Olsen Thielen and has more than 35 years experience in the telecommunications industry, including working at Qwest.



### **Experience**

- Extensive experience in ILEC, CLEC, Wireless and VoIP Interconnection negotiations, telecommunications and information service market and product management, financial analysis and planning, billing, budgeting, strategic planning and exchange sales planning and implementation.
- Testifies before state Public Service Commissions.
- Prepares and assists in regulatory filings and tariff consultations.

### **Core Specialization**

Telecommunications related companies (ILEC, CLEC, Internet, wireless, wireless broadband, VoIP and cooperatives)

**Olsen Thielen**  
2675 Long Lake Road  
St. Paul, MN 55113-1117

**Phone:**  
651-621-8631

**Fax:**  
651-483-2467

**E-Mail:**  
[pholton@otcpas.com](mailto:pholton@otcpas.com)

**Website:**  
[www.otcpas.com](http://www.otcpas.com)

### **Education and Affiliations**

Bachelor of Science in Engineering from South Dakota State University, Brookings  
Master of Business Administration, University of Nebraska, Omaha

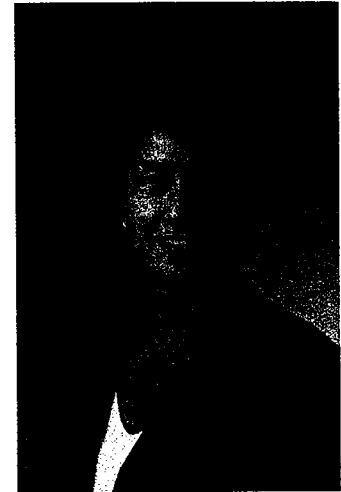
### **Other Executive/ Specialized Training Programs**

Extensive Telephony and Data Solutions Training,  
Qwest Communications  
Managing Strategic Alliances, Wharton School of Business  
Developing Ventures for Competitive Effectiveness,  
Wharton School of Business  
Executive Program in Market Management, Columbia Business School  
21st Century Program on Quality, University of Minnesota  
Executive Program

Cecilia Ray works in the areas of telecommunications law, utility regulation, commercial real estate and general corporate and business law. Her experience in representing clients includes:

- Negotiating and drafting agreements for business operations, acquisitions, sales and leases
- Advising businesses in structuring transactions and contract terms
- Working with lenders and borrowers involved in complex commercial financing transactions
- Representing public utilities and telecommunications service providers in regulatory proceedings

Ms. Ray is a member of the American, Minnesota State and Hennepin County Bar Associations.



**Cecilia Ray**

**Phone**  
612-877-5289

**Fax**  
612-877-5999

**Email**  
rayc@moss-barnett.com

**AREAS OF PRACTICE:**

Commercial Real Estate

General Corporate and  
Business Law

Telecommunications Law

Utility Regulation

**BAR ADMISSIONS:**

Minnesota

**EDUCATION:**

University of Minnesota Law School, Minneapolis, Minnesota, 1985

J.D.

Honors: Cum Laude

University of Minnesota, 1982

B.A.

**PROFESSIONAL ASSOCIATIONS AND MEMBERSHIPS:**

Hennepin County Bar Association

Member

Minnesota State Bar Association

Member

American Bar Association

Member

Attorneys in Moss & Barnett's Communications group collectively have more than 100 years of experience in representing the unique legal and regulatory interests of communications companies, with a concentration on rural incumbent local exchange carriers ("Rural ILECs") and competitive local exchange carriers ("CLECs").

We have provided legal, regulatory and government affairs services to our communications clients in:

- Iowa
- Minnesota
- New Mexico
- North Dakota
- Oklahoma
- South Dakota
- Texas
- Washington
- Wisconsin
- Before the Federal Communications ("FCC")

One of our group members also concentrates his practice in governmental matters related to cable television regulation on a national basis.

While our representation has taken many different forms, the core of our experience is in addressing:

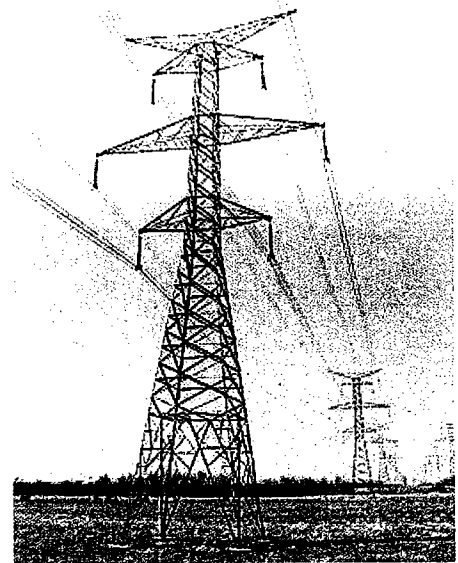
- Intercarrier compensation issues, negotiations and disputes

## Communications

**Phone**  
612-877-5000

**Fax**  
612-877-5999

**Email**  
[contact@moss-barnett.com](mailto:contact@moss-barnett.com)



- Unbundled network element cost cases and other matters arising under the Telecommunications Act of 1996 State telecommunications certifications
- ETC certifications
- Regulatory investigations and complaints, including earnings issues and disputes arising under the Telecommunications Act of 1996

The wide range and depth of our experience enables us to integrate specific legal, regulatory and government affairs projects into a client's broader objectives. For example, we have:

- Recently negotiated a traffic identification agreement with Qwest for phantom traffic terminated over Qwest access tandems
- Provided legal support resulting in the recovery of lost access revenues from two major IXCs who were terminating unidentified traffic through third-party CLECs
- Provided legal representation and support for CLECs in numerous unbundled network element (UNE) cost cases, wholesale service performance disputes and other proceedings arising under the Telecommunications Act of 1996 (preparing filings, pleadings, testimony, cross examination, briefs and oral argument)
- Represented CLECs in state and federal court appeals related to an array of disputes, including matters related to UNE pricing, wholesale service performance standards and Intercarrier Compensation
- Provided direction and drafted extensive comments on behalf of a coalition of Rural ILECs in response to various access and universal service related proceedings before the FCC

- Provided legal representation and support in numerous access "reform" proceedings (preparing filings, pleadings, testimony, cross examination, briefs, oral argument and negotiations)
- Negotiated several dozen interconnection agreements, including agreements with CMRS providers
- Provided legal representation and support in proceedings for intercarrier compensation in ELC and EAS circumstances
- Represented several groups of Rural ILECs in connection with ETC applications by CMRS providers in rural telephone company service areas
- Represented Rural ILECs in numerous rate cases, earnings investigations and proceedings to establish individual regulatory plans
- Handled a large number of individual traffic exchange matters
- Obtained the legal and regulatory consent for numerous sales, acquisitions and mergers of telecommunications companies

In addition to our regulatory/intercarrier negotiation experience, Moss & Barnett also provides business and corporate legal services to our telecommunications clients.