

Identity Theft “Red Flags” Rules Under the FACT Act

Andrew Smith, Morrison & Foerster LLP

May 15, 2008

Background to New Requirements

- **Fair and Accurate Credit Transactions (“FACT”) Act**
- **During FACT Act legislative process, Congress was concerned about several emerging issues**
 - **Including increasing incidence of identity theft**
- **New obligations for lenders and others to prevent, detect, and mitigate ID theft**

- **Expansive definition of “credit”**
 - **Any deferral of payment**
 - **12 C.F.R. § 202.2(j)**
 - **Can include telecom, utilities, invoicing, subscriptions**
- **Expansive definition of “creditor”**
 - **Anyone who participates in credit decision**
 - **12 C.F.R. § 202.2(l)**
 - **Can include brokers, arrangers**

Key FCRA Definitions

- **Expansive definition of “identity theft”**
 - **Includes new accounts and existing accounts**
 - **Includes attempted identity theft**
 - **Includes the “identity” of a business**
 - **16 C.F.R. § 603.2**
- **Definition of “red flag” narrower than proposed**
 - **Indicator of “possible existence of ID theft”**

- **Three segments of final Rule**
 - **The Rule itself: covered entities must develop written ID theft prevention program**
 - **Accompanying Guidelines: must be considered when developing program**
 - **Appendix J: may consider list of red flags possibly indicating ID theft**

Red Flags Rule

- **Mandatory compliance date Nov. 1, 2008**
- **Preempts state law requirements**
 - **With respect to “conduct required by” FCRA section 615(e)**

“Covered Accounts”

- **Entities must determine whether they offer or maintain “covered accounts”**
- **Consumer accounts involving multiple payments or transactions are always “covered accounts”**
 - **Credit cards, checking accounts, mortgage loans**
- **Other accounts if reasonably foreseeable fraud or ID theft risk to customers or institution itself**

“Covered Accounts”

- **Business accounts also may be “covered accounts”**
 - **Such as small business, sole proprietors**
 - **If there is a “reasonably foreseeable risk” to customers or to safety and soundness from identity theft**
 - **Risk = financial, operational, compliance, reputation, or litigation**

“Covered Accounts”

- **Benefit of preemption for business accounts**
- **In making this risk determination, entity must consider -**
 - **Methods it uses to open accounts**
 - **Methods available to access accounts**
 - **Previous experiences with ID theft for that product or for other products**

- **All depository institutions and creditors that offer “covered accounts” must establish a program**
- **Much work has already been done -**
 - **GLBA data security, section 326 USA PATRIOT Act, AML/BSA programs**
 - **But must combine into a single written program**

- **Entities that offer or maintain covered accounts must**
 - **Develop and implement a WRITTEN identity theft prevention program that is designed to**
 - **Prevent, detect, and mitigate ID theft in**
 - **New accounts and**
 - **Existing accounts**
- **Must include policies and procedures to**
 - **Identify relevant red flags**
 - **Detect those red flags**
 - **Respond when red flags are detected**
- **Must be updated periodically to reflect new risks**

- **Must be approved by the Board or committee of the Board**
- **Must be overseen by senior management**
- **Must include staff training and oversight of service providers**
- **Must consider the Guidelines provided by the agencies**
- **Must be updated to consider new threats as they arise**

- **Guidelines, 12 CFR pt. 222, App. J, are a “cookbook”**
- **Provide agency guidance on**
 - **Identifying red flags**
 - **Detecting red flags**
 - **Preventing and mitigating ID theft**
 - **Administering the program**

- **The guidance provided is important because Rule will be enforced based on this guidance**
- **Enforcement**
 - **No private right of action**
 - **Administrative enforcement only is appropriate, given flexible, risk-based requirements**

Guidelines: Identifying Red Flags

- **“Should consider”**
 - **Types of covered accounts they offer or maintain**
 - **Methods of opening and accessing such accounts**
 - **Previous experiences with ID theft**
- **Should incorporate red flags from**
 - **Entity’s own experience**
 - **New methods of ID theft**
 - **“Applicable supervisory guidance”**
- **Also may consider list of possible red flags prepared by agencies**

***Must* consider four major categories and *may* consider examples identified for each**

- 1. Alerts and notifications received from credit bureaus and third-party service providers**
 - **Examples: fraud alerts, address discrepancy notices, credit freeze, and unusual patterns of activity on credit report**
- 2. Presentation of suspicious documents or suspicious identifying information**
 - **Examples: IDs that appear altered or forged, inconsistent ID information, invalid SSN, address is mail drop**
- 3. Unusual or suspicious account usage patterns**
 - **Examples: changes in account usage or purchase of jewelry and electronics**
- 4. Notice from customer, ID theft victim, or law enforcement**

***Note:* Compliance officers should refer to the full list of examples at 12 CFR pt. 222, App. J, Supp. A**

- **Verify the identity of a person opening a covered account**
- **And, in the case of existing covered accounts**
 - **Authenticate customers**
 - **Monitor transactions**
 - **Verify validity of change-of-address requests**
 - **Action taken should be commensurate with the risk of ID theft**

- **Provide for appropriate responses to red flags that are commensurate with risk presented**
 - Consider aggravating factors, such as data security breach or phishing
- **Possible appropriate responses**
 - Monitoring account
 - Contacting customers
 - Changing passwords or PINs
 - Closing account or assigning new account number
 - Not opening a new account
 - Not attempting to collect, or not selling/assigning account
 - Notifying law enforcement
 - Determining no response is necessary
- **12 CFR pt. 222, App. J**

- **Board of directors or senior management**
 - **Assign specific responsibility for implementation**
 - **Review reports by staff**
 - **Approve material changes to program**

- **Staff report *at least annually* on**
 - **Effectiveness of policies**
 - **Service provider arrangements**
 - **Significant security incidents**
 - **Recommendations for material changes**

- **Ensure by written contract that service providers**
 - **Perform designated activities for covered accounts**
 - **Implement procedures to detect, prevent, and mitigate ID theft**
- **Update program as necessary**

For Further Information Contact:

Ken Markison, Mortgage Bankers Association,
(202) 557-2930 or kmarkison@mortgagebankers.org

Andrew Smith, Morrison and Foerster
(202) 887-1558 or andrewsmith@mof.com