ID Theft Red Flags Rule Implementation Challenges

Jo Ann Maddox
MWR IT Manager

Office of Thrift Supervision

June, 2008

Agenda

- Key Elements of the Red Flags Rule
  - WHO wrote the Rule?
  - WHAT you must do to comply with the Rule.
  - DEFINITIONS and a possible concern.
  - WHEN you must be compliant.
- Risk Based Regulation
- Red Flags Rule Guidelines
- Supplement to Red Flags Rule
- Red Flags Rule Implementation Challenges

Key Elements of Red Flags Rule

- FFIEC agencies and FTC released final rule in November 2007
  - Implements sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003
  - Defined “red flag” as “a pattern, practice, or specific activity that indicates the possible existence of identity theft”
  - Agencies received 129 comment letters on proposal
  - Complex interagency process with five federal depository institution regulators plus the FTC
  - Rule applies to both regulated and non-regulated entities

Key Elements of Red Flags Rule

- Outlines steps financial institutions and creditors must take to administer the Program:
  - Obtain approval of the initial written Program
  - Ensure oversight of the development
  - Implementation and overseeing service provider arrangements
  - Train staff, as necessary, to effectively implement the Program

Key Elements of Red Flags Rule

- Broad definition mandated by the law: “the risks of identity theft to a customer may include ‘financial, reputation and litigation risks that occur when another person uses a customer account fraudulently, such as by using the customer credit card number to make unauthorized purchases.’ ”
  - Key Concern: By defining identity theft as using customer credit card numbers to make unauthorized purchases, the rule confuses fraud (lost, stolen, counterfeit cards/numbers) with true identity theft, such as true name fraud or account takeover

Key Elements of Red Flags Rule

- Final rule consists of three parts:
  - Risk-Based Regulation
  - Guidelines
  - Supplement
- Regulation and guidelines go into effect on January 1, 2008
  - Compliance required by November 1, 2008

Key Elements of Red Flags Rule

1. Risk Based Regulation:
   - Requires each institution/creditor that holds consumer accounts, or any other account for which there is a reasonably foreseeable risk of identity theft, to implement a written identity theft prevention program for new and existing accounts
   - Identify relevant patterns, practices, and specific forms of activity
   - Respond to red flags and incorporate into program
   - Update program & Train staff

Key Elements of Red Flags Rule

2. Guidelines
   - More detailed
   - Intended to assist financial institutions in formulating a program that satisfies the requirements of the rule
   - Describes the risk factors that financial institutions and creditors should consider when identifying:
     - Relevant red flags
     - Sources of red flags
     - Methods to prevent/mitigate ID theft

Key Elements of Red Flags Rule

3. Supplement
   - Includes 26 “illustrative” red flags in five categories:
     - Alerts from a consumer reporting agency
     - Suspicious documents
     - Suspicious personal identifying information
     - Suspicious activity in connection with a covered account
     - Notice of suspicious activity in connection with a covered account

Implementation Challenges

- No “Silver Bullet” in Tackling ID Theft
- Flexibility is Important
  - Fraudsters constantly change tactics and financial institutions need the flexibility to respond to these changes
    - A set list of red flags today may not be relevant in the future as fraudsters develop new tactics
  - Large, complex financial institutions typically have multiple lines of business with responsibility for managing fraud
    - Variations in response programs & training programs

Implementation Challenges

- Integration with Existing Programs
  - Preamble of rule notes that an institution's identity theft prevention program may incorporate or cross-reference aspects of their security program and that an institution's customer identification program could be incorporated
  - No requirement that identity theft program be identical across different lines of business

Implementation Challenges

- Management Oversight
  - Striving for reasonable compliance program
    - Substantial risk of creating a bureaucratic morass by a compliance driven process that has the potential for creating a “parallel universe” within large financial institutions
    - Coming to terms with what is “reasonable”?
  - Seeking collaboration with lines of business, fraud, and information security
  - Opportunity for some firms to implement enterprise-wide fraud risk management program
  - Avoid “reinventing the wheel” by adapting current, successful programs

Implementation Challenges

- Documentation of program
  - Current processes already in place although many are not formally documented
- M&A impact
- Economic pressures

Implementation Challenges

- Vendor Management
  - Outlining needs
  - Negotiating contracts
  - Impact on auditing programs

- Budget/Procurement Cycle
  - 11/2008 deadline a challenge for some large firms to incorporate in technology budget cycle

Implementation Challenges

- Securing Board Approval
- Consistency in Regulatory Oversight
  - Examination Procedures (in development):
    - Impact of consumer compliance vs more risk-based IT driven process

Contact Info

Jo Ann Maddox
IT Examinations Manager
OTS Midwest Regional Office
Email: joann.maddox@ots.treas.gov
Tel: (979) 221-4208