# The FACT Act – An Overview

## The FACT Act

# An Overview of the Final Rulemaking on Identity Theft Red Flags and Address Discrepancies

**Pavneet Singh & Tiffany George**
*Attorneys, Division of Privacy and Identity Protection*
**Federal Trade Commission**

# Outline of Presentation

- Identity Theft Red Flag Rules
- Identity Theft Red Flag Guidelines
- Rule on Address Discrepancies
- Questions

# Statutory Provisions Implemented

- FACT Act amended the Fair Credit Reporting Act (FCRA)

- Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act)

Rules: 72 Fed. Reg. 63718 (November 9, 2007)
http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf

# Background

- Joint rulemaking
- Final rules published November 9, 2007
- Full compliance required by November 1, 2008

# Identity Theft Red Flags

FACT Act Section 114

FCRA Section 615(e)

12 CFR 41.90 and 41.91

# Identity Theft Red Flags

- Risk-based final rule
- Guidelines
- Supplement (26 examples of red flags)

# 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

# Definitions

**A "financial institution" is:**

- A state or national bank
- A state or federal savings and loan association
- A mutual savings bank
- A state or federal credit union, or
- Any other person that directly or indirectly holds a transaction account belonging to a consumer

# Definitions (cont'd)

**A "creditor" is:**

- Any person who regularly extends, renews, or continues credit
- Any person who 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

# Definitions (cont'd)

**A "covered account" is:**

- A consumer account designed to permit multiple payments or transactions, or
- Any other account for which there is a reasonably foreseeable risk from identity theft

# 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
- Ensure the Program is updated periodically to address changing risks

# Administration of the Program

- Obtain approval of the initial Program by the board or a committee thereof
- Ensure oversight of the Program
- Train appropriate staff
- Oversee service provider arrangements

# Consideration of the Guidelines

**Rules require:**

- Consideration of the Guidelines
- Incorporation of appropriate Guidelines into the Program

# Identity Theft
# Red Flag Guidelines

# Overview of the Guidelines

I. Incorporate existing policies and procedures
II. Identify relevant red flags
III. Procedures to detect red flags
IV. Appropriate responses to red flags
V. Periodic updating of the Program
VI. Administering the Program
VII. Other legal requirements

# I. Incorporate Existing Policies and Procedures

- Existing anti-fraud program
- Customer identification program (CIP)
- Information security program

# II. Identify Relevant Red Flags

**Risk factors for identifying relevant red flags are:**

- Types of covered accounts offered or maintained
- Methods provided to open or access covered accounts
- Previous experiences with identity theft

# II. Identify Relevant Red Flags (cont'd)

**Sources of red flags are:**

- Incidents of identity theft that have been experienced
- Methods of identity theft reflecting changes in identity theft risks
- Applicable supervisory guidance

# II. Identify Relevant Red Flags (cont'd)

## Five categories of red flags are:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers
- Presentation of suspicious documents
- Presentation of suspicious personal identifying information
- Unusual use of, or other suspicious activity related to, a covered account
- Notice from customers, victims of identity theft, or law enforcement authorities

# III. Procedures to Detect Red Flags

- Verify identity
- Authenticate customers
- Monitor transactions
- Verify validity of address changes

# IV. Appropriate Responses to Red Flags

- Monitor accounts
- Contact customer
- Change passwords
- Close and reopen account
- Refuse to open account
- Don't collect on or sell account
- Notify law enforcement
- No response

# V. Periodic Updating of the Program

- 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

# VI. Administering the Program

## Oversight of the Program involves:

- Assigning specific responsibility
- Reviewing reports
- Approving material changes in the Program

# VI. Administering the Program (cont'd)

**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

# VI. Administering the Program (cont'd)

## Oversight of service providers:

- 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

# VII. Other Legal Requirements

- Suspicious Activity Reports (SARs)
- Other FCRA provisions

# Examples of Red Flags

- Warning from consumer reporting agencies

  ⇨Fraud or active duty alert included in consumer report

- Suspicious documents

  ⇨Documents provided for identification appear to be altered

- Suspicious personal information

  ⇨Inconsistent with external information sources

# Examples of Red Flags (cont'd)

- Unusual use of account

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

- Notice from customers

⇨Customer notifies bank of unauthorized charges

# Enforcement of Red Flags Rules

- Administrative enforcement under 12 USC 1818
- No private right of action
- State Attorneys General
- No criminal penalties

# Rule on Notices of Address Discrepancy

# Notices of Address Discrepancy

FACT Act Section 315

FCRA Section 605(h)

12 CFR 41.82

# Notices of Address Discrepancy

Duties of users of consumer reports that receive a "notice of address discrepancy" from a nationwide consumer reporting agency (NCRA as defined in FCRA)

# Notices of Address Discrepancy

**"Notice of address discrepancy" notifies the user of a substantial difference between:**

- Address the user provided, and
- Address in the NCRA's files

# Notices of Address Discrepancy

**Regulatory Requirement:**

The user must have reasonable policies and procedures to establish a reasonable belief that the consumer report relates to the consumer about whom the report was requested

# Notices of Address Discrepancy

## Establishing a reasonable belief — Examples

- Compare information in the consumer report to information the user:
  - Maintains in its records
  - Obtains from third-party sources
  - Obtained to comply with CIP rules
- Verify information in the consumer report with the consumer

# Notices of Address Discrepancy

**Regulatory Requirement:**

The user must have reasonable policies and procedures to furnish a confirmed address for the consumer to the NCRA, when the user:

- Can form a reasonable belief that the report relates to the consumer
- Establishes a continuing relationship with the consumer
- Regularly furnishes information to the NCRA

# Questions???