FIGHTING FRAUD WITH THE RED FLAGS RULE & ENSURING ACCURACY WITH THE ADDRESS DISCREPANCY RULE

Tiffany George
Attorney, Division of Privacy & Identity Protection
Federal Trade Commission

WHAT'S ON YOUR MIND

- So what is the Red Flags Rule?
- Who's covered by the Red Flags Rule?
- If we're covered by the Red Flags Rule, what do we need to do?
- How do we design an Identity Theft Prevention Program?
- What are the Red Flag Guidelines?
- What about the Address Discrepancy Rule?

THE FACT ACT

Fair and

Accurate

Credit

Transactions Act of 2003

amending the
Fair Credit Reporting Act (FCRA)

RULES: 72 Fed. Reg. 63718 (November 9, 2007)
www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf
(FTC Rules p.63771-63773, Guidelines p. 63773-63774, Supplement p. 63774)

BACKGROUND

- Joint rulemaking
- Final rules published November 9, 2007
- Compliance required by November 1, 2008, but enforcement forbearance for the Red Flags Rule until May 1, 2009, for entities under FTC jurisdiction

SO WHAT IS THE RED FLAGS RULE?



RED FLAGS RULE

- FACT Act Section 114
- FCRA Section 615(e)
- 16 C.F.R. § 681.2

PURPOSE OF THE RED FLAGS RULE

- To ensure that your business or organization is on the lookout for the signs that a crook is using someone else's information, typically to get your products or services with no intention of paying.
  - A "red flag" is a pattern, practice, or specific activity that could indicate identity theft
- It's not just another data security regulation.

STRUCTURE OF THE RED FLAGS RULE

- Risk-based rule
- Guidelines (Appendix A)
- Supplement A – 26 examples of red flags

WHO'S COVERED BY THE RED FLAGS RULE?



WHO'S COVERED BY THE RED FLAGS RULE?

- Financial institutions
- Creditors

WHO'S COVERED BY THE RED FLAGS RULE?

From the FCRA, 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

* From the Federal Reserve Act, Section 19(b) – an account that allows withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or similar items to make payments or transfers to third persons or others

WHO'S COVERED BY THE RED FLAGS RULE?

From the ECOA, 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
  - A "person" means "a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association."
  - "Credit" means an arrangement by which you defer payment of debts or accept deferred payments for the purchase of property or services.

IF WE'RE COVERED BY THE RED FLAGS RULE, WHAT DO WE NEED TO DO?



IF WE'RE COVERED BY THE RED FLAGS RULE, WHAT DO WE NEED TO DO?

- Financial institutions and creditors must conduct a periodic risk assessment to determine if they have "covered accounts."
- If they do, they must develop, implement, and administer 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.

IF WE'RE COVERED BY THE RED FLAGS RULE, WHAT DO WE NEED TO DO?

An "account" is:

- A continuing relationship established by a person with an FI or creditor to obtain a product or service for personal, household, or business purposes.

IF WE'RE COVERED BY THE RED FLAGS RULE, WHAT DO WE HAVE TO DO?

A "covered account" is:

- A consumer account designed to permit multiple payments or transactions, and
- Any other account for which there is a reasonably foreseeable risk from identity theft
  - Risk factors
    1. Methods provided to open the account
    2. Methods provided to access the account
    3. Previous experiences with identity theft

HOW DO WE DESIGN AN IDENTITY THEFT PREVENTION PROGRAM?



DESIGNING YOUR PROGRAM

Develop reasonable processes and procedures for :

- STEP #1 – Identify relevant red flags. Identify the red flags you're likely to come across in your business that indicate a crook is using someone else's information to get your products or services with no intention of paying.
- STEP #2 – Detect red flags. Set up procedures to detect them in your day-to-day operations.
- STEP #3 – Prevent and mitigate identity theft. When you spot the red flags you've identified, respond appropriately to prevent and mitigate harm.
- STEP #4 – Update your Program. The risks of identity theft can change rapidly, so keep your Program current and educate your staff.

DESIGNING YOUR PROGRAM

The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

USING THE GUIDELINES

The Rules require you to:

- Consider the Guidelines
- Incorporate appropriate Guidelines into your Program

ADMINISTERING YOUR PROGRAM

- Get approval of the initial Program from your Board of Directors or from a committee of the Board
- After that, the Board may designate a senior management employee to oversee:
  - Development, implementation, and administration of the Program
  - Training of appropriate staff
  - Arrangements with service providers

WHAT ARE THE IDENTITY THEFT RED FLAGS GUIDELINES?



RED FLAGS GUIDELINES

1. Incorporate existing policies and procedures.
2. Identify relevant red flags.
3. Set up procedures to detect red flags.
4. Respond appropriately to red flags.
5. Update your Program periodically.
6. Administer your Program.
7. Consider other legal requirements.

Incorporate existing policies and procedures

- Evaluate your existing anti-fraud programs
- Evaluate your information security programs

Identify relevant red flags

- Risk factors:
  - Types of covered accounts you offer or maintain
  - Methods for opening or accessing covered accounts
  - Previous experience with identity theft
- Sources of red flags:
  - Episodes of identity theft that have already happened
  - Changes in how crooks are committing identity theft
  - Applicable supervisory guidance

Identify relevant red flags

- Five categories of red flags*:
  - Alerts, notifications, or other warnings received from credit reporting agencies or service providers
  - Suspicious documents
  - 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

* 26 examples are found in Supplement A

Set up procedures to detect red flags

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

Respond appropriately to red flags

- Monitor accounts
- Contact customer
- Change passwords
- Close and reopen account
- Refuse to open account
- Don’t sell the account or collect on it against the identity theft victim
- Notify law enforcement
- In some cases, no response may be warranted

Update your Program periodically in light of:

- 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

Administer your Program

- Oversight of the Program by your Board or a senior manager involves:
  - Assigning specific responsibility for implementation
  - Reviewing reports
  - Approving materials changes to your Program.

Administer your Program

- At least once a year, the Board or the senior manager should get a report addressing material matters like:
  - Service provider arrangements
  - Whether your policies and procedures have been effective in addressing the risk of identity theft in connection with covered accounts
  - Significant incidents involving identity theft and management's response
  - Recommendations for changes to the Program

Administer your Program

- Oversight of your service providers involves ensuring their activities are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

Other legal requirements

- Other FCRA provisions – for example, information furnisher duties to update or correct inaccurate information, and not report inaccurate information (15 U.S.C. 1681s-2)

EXAMPLES OF RED FLAGS (SUPP. A)

- Warning from credit 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 (SUPP. A)

- Unusual use of account → **Account used in a way inconsistent with historical patterns of activity**
- Notice from customers → **Customer notifies you about identity theft**

WHAT ABOUT THE ADDRESS DISCREPANCY RULE?



ADDRESS DISCREPANCY RULE

- FACT Act Section 315
- FCRA Section 605(h)
- 16 CFR § 681.1

WHO'S COVERED?

- Users of credit reports

NOTICE OF ADDRESS DISCREPANCY

"Notice of address discrepancy" comes from a nationwide credit reporting agency and notifies the user of a substantial difference between:

- Address the user provided, and
- Address in the credit reporting company's files

➢ "Nationwide credit reporting agency" (NCRA) – as defined in FCRA

ENSURING ACCURACY

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

REASONABLE BELIEF

Establishing a "reasonable belief" — examples

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

CONFIRMING ADDRESS

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

ENFORCEMENT OF RULES

- Administrative enforcement under 15 U.S.C. 1681s (Section 621 of the FCRA).
- No private right of action for 16 C.F.R. 681.2
- State Attorneys General
- No criminal penalties

QUESTIONS?

RedFlags@ftc.gov

www.ftc.gov