

New Identity Theft Rules, Red Flags and Address Discrepancies 16 C.F.R. 681

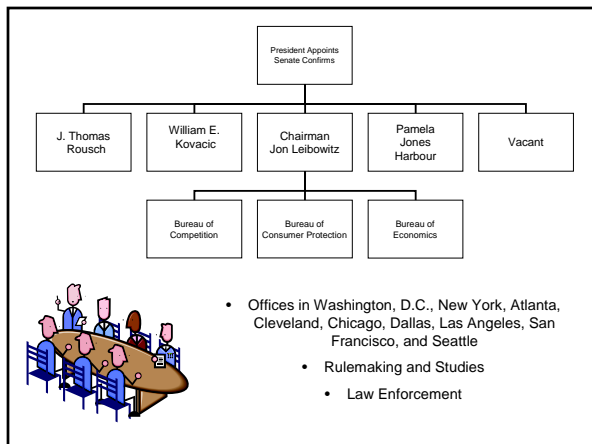
72 Fed. Reg. No. 217 (Nov. 9, 2007) p. 63718
<http://www2.ftc.gov/opa/2007/10/redflag.shtm>

Jonathan L. Kessler
Federal Trade Commission
1111 Superior Ave., Suite 200
Cleveland, Ohio 44114
216-263-3436
jkessler@ftc.gov

I. Overview of the FTC

II. Evolution of Privacy Laws

III. Red Flags and Address Discrepancy Rules



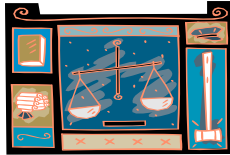
Major FTC Statutes

- **FTC Act** – Prohibits Unfair Methods of Competition and Unfair or Deceptive Acts or Practices, 15 U.S.C. 41
- **Credit-Related Statutes**
 - Fair Credit Reporting Act (FCRA) / Fair and Accurate Credit Transactions Act (FACTA, 2003), 15 U.S.C. 1681
 - Equal Credit Opportunity Act, 15 U.S.C. 1691
 - Truth-in-Lending Act, 15 U.S.C. 1601
 - Fair Debt Collection Act, 15 U.S.C. 1692
- **Other Statutes**
 - Hart-Scott-Rodino Act (Merger Notice), 15 U.S.C. 1311
 - Magnusson-Moss (Warranties), 15 U.S.C. 2301



FTC Rules

- * Force of a Statute
- * Costly to violate



- | | |
|---|--|
| <ul style="list-style-type: none"> • Identity Theft Rules (Red Flags, Address Discrepancies, Duties of Card Issuers & Changes of Address) • Insulation Testing • Telemarketing & Do Not Call | <ul style="list-style-type: none"> • Sales of Franchises and Business Opportunities • Door-to-Door Sales (Cooling-Off Rule) • Used Car Rule • Eyeglass Prescriptions |
|---|--|

Enforcement Options and Remedies

- **Administrative Actions:** Trial before an ALJ, Review by the Commission, Appeal to Courts of Appeals & Supreme Court
 - Remedy – Cease and Desist Order
 - Antitrust and some Advertising cases



- **Federal Court:** Trial in District Court, Appeal to Courts of Appeal & Supreme Court
 - Section 5 Fraud, Rules, and other Statutory violations
 - Remedies include injunctions, consumer redress, disgorgement, bans, bonds, and civil penalties



Civil Penalties For Red Flags Rule Violations

- Commission brings a law enforcement action in U.S. District Court
- Must prove a knowing violation which constitutes a pattern or practice of FACTA violations
- Maximum of \$3500 per violation
- Civil Penalty is set by the judge after considering
 - Degree of culpability
 - History of prior conduct (previous offenses or warnings)
 - Ability to Pay
 - Effect on ability to continue to do business
 - Such other matters as justice may require



Enforcement of Red Flags Rules

- Enforcement by FTC unless offender is a bank, savings & loan, credit union, or air carrier, or regulated by the Surface Transportation Board or the Secretary of Agriculture
- No private right of action
- State Attorneys General
- No criminal penalties

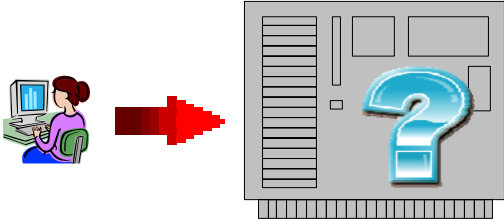


An Abbreviated History of Privacy Statutes

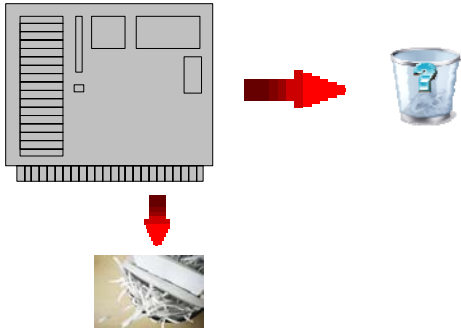
- 1997 and before: The Wild West of the Internet



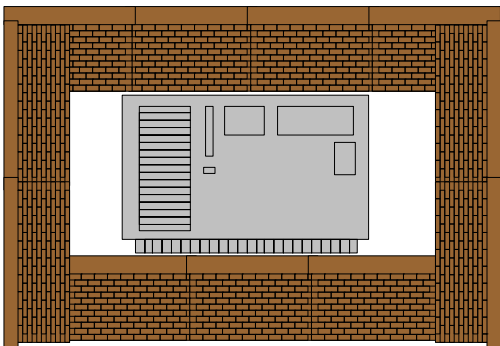
Disclosure:
Fair Information Practice Principles
Gramm-Leach Bliley Act




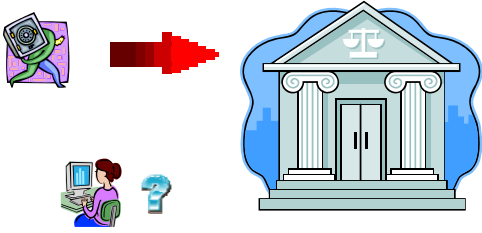
GLB and FACTA Disposal Rules



TJX



Identity Theft (Red Flags) Rule 



Three Rules in One
 16 C.F.R. Part 681

- 681.1 – Address Discrepancies
- 681.2 – Red Flags
- 681.3 – Duties of Credit/Debit Card Issuers wrt Address Changes

A Break From the Past

- Concern is not just keeping an organization's data safe but keeping an identity thief from getting goods/services from the organization (2d level theft)
- FTC to enforce against utility companies, medical facilities, & telecommunications companies, inc. gov't-run entities

**Red Flags Rule (681.2)
 Structure**

- Identity Theft Red Flags Rule
- Identity Theft Red Flags Guidelines
- Examples of Red Flags

(When in doubt, start at the back & move forward)

RFR in One Sentence

"Financial institutions" and "creditors" with covered accounts" must implement a written **Identity Theft Prevention Program** to *detect, prevent, and respond* to **identity theft** in connection with new or existing "covered accounts."

- "Financial Institution" – a bank, savings & loan, credit union, or other entity that holds consumers' transaction accounts
- "Creditor" (from the ECOA) – an entity who (1) extends, renews or continues credit, (2) arranges credit, or (3) is the assignee of an original creditor
- "Credit" (also from ECOA) – Right to defer payment
- "Covered Account" – (1) An account designed for multiple transactions or payments or (2) for which there is a reasonably foreseeable risk from identity theft

RFR in One Sentence

"Financial institutions" and "creditors" with covered accounts" must implement a written Identity Theft Prevention Program to *detect, prevent, and respond* to **identity theft** in connection with new or existing "covered accounts."

What the Program must do:

- 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
- Adjustment Provisions – Review and change as risks and information change

RFR in One Sentence

Financial institutions and creditors with covered accounts "must develop and implement a written Identity Theft Prevention Program (Program) that is designed to *detect, prevent, and respond* to identity theft" in connection with new or existing "covered accounts."

Detect – Identifying Relevant Red Flags (Guidelines)

- Incorporate existing anti-fraud, customer identification, and information security practices into the Program Guidelines, Part I
- "Risk Factors," Guidelines, Part II(a)
 - Experience with Identity Theft
 - Types of "covered accounts" (e.g., depository v. credit)
 - How "covered accounts" are opened (e.g., phone, mail, internet, or in-person)
 - How "covered accounts" are accessed (e.g., phone, internet, or in-person)
- "Sources" of Red Flags, Guidelines, Part II(b)
 - Experience with Identity Theft
 - Press/third party reports of Identity Theft
 - Changes in risk over time
 - Supervisory guidance

RFR in One Sentence

Financial institutions and creditors with covered accounts "must develop and implement a written Identity Theft Prevention Program (Program) that is designed to **detect, prevent, and respond** to identity theft" in connection with new or existing "covered accounts."

Detect – Identifying Relevant Red Flags (Guidelines)

- "Categories of Red Flags," Guidelines, Part II(c)"
 - Warnings from credit bureaus or other service providers such as fraud detection services;
 - Suspicious documents
 - Suspicious personal identifying information, such as a suspicious address change
 - Unusual or suspicious use of an account
 - Notice from a customer, ID theft victim, or someone else of possible identity theft in connection with a covered account

Use the Risk Factors, Sources, and Categories in the Guidelines as appropriate to your organization

RFR in One Sentence

Financial institutions and creditors with covered accounts "must develop and implement a written Identity Theft Prevention Program (Program) that is designed to **detect, prevent, and respond** to identity theft" in connection with new or existing "covered accounts."

Detect – Detecting Red Flags (Guidelines Part III)

- Obtaining identifying information about persons opening new covered accounts, perhaps by using the Customer Identification Program rules in 31 C.F.R. 103.121
- Authenticating customers, monitoring transactions and verifying address changes for existing covered accounts

RFR in One Sentence

Financial institutions and creditors with covered accounts "must develop and implement a written Identity Theft Prevention Program (Program) that is designed to **detect, prevent, and respond** to identity theft" in connection with new or existing "covered accounts."

Preventing and Mitigating Identity Theft – some Responses when Red Flags pop-up (Guidelines, Part IV)

- Monitor a covered account for evidence of ID Theft
- Contact your customer
- Change passwords that permit access to a covered account
- Reopen the covered account
- Decline to open a new covered account
- Close an existing account
- Stop collection efforts on an existing account
- Notify law enforcement agencies
- Do nothing

RFR in One Sentence

Financial institutions and creditors with covered accounts "must develop and implement a written Identity Theft Prevention Program (Program) that is designed to **detect, prevent, and respond** to identity theft" in connection with new or existing "covered accounts."

Update the Program as necessary (Guidelines, Part V)

- Experiences of the organization with ID theft
- Changes in how identities are stolen
- New methods of detecting, preventing, or mitigating identity theft
- Changes in the organization's covered accounts
- Changes in the business structure of the organization (e.g., mergers, acquisitions, alliances, or new service provider agreements)

Program Administration

- Approval of the initial Program by the board of directors or a committee of the board
 - Does a municipal government have to have the plan approved by the governing council, or is a mayor or city manager sufficient?
- Involve the Board, a committee of the board, or senior management in the oversight, development, implementation, and administration of the Program
- Train Staff as necessary
- Oversee service providers (e.g., billing agents or debt collectors)

**Administration (Continued)
(Guidelines Part VI)**

- Assign responsibility for Program implementation
- Periodic (at least annual) reports to the Board or Sr. Management in charge on Program operation regarding
 - Effectiveness of existing policies and procedures
 - Service provider arrangements
 - Major incidents of identity theft
 - Suggested changes to the Program
 - Other material issues
- Supervise Service Providers – make sure they have policies and procedures to detect, prevent, and mitigate ID theft that may occur in connection with SP's activities
 - Contract provisions requiring the SP to have a Program to detect RF and (1) report to the organization or (2) take direct steps to mitigate
 - Require the SP to disclose its RF Program to your organization (JLK)

Don't Forget -- Other Legal Requirements

- 15 U.S.C. 1681c-1(h) (FCRA) – Extending credit to consumers with alerts (fraud or active-duty) on their credit reports
- 15 U.S.C. 1681s-2 – Obligations of organizations to furnish credit bureaus accurate and current information
- 15 U.S.C. 1681m(f) – Prohibition on sending debts caused by ID theft to debt collectors

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

Address Discrepancies
16 C.F.R. 681.1

When the Rule Applies

- User of consumer reports receives a “notice of address discrepancy” from a nationwide consumer reporting agency (NCRA as defined in the Fair Credit Reporting Act)

- “Notice of address discrepancy” notifies of a substantial difference between
 - Address the User provided the NCRA and
 - Address in the NCRA’s files

Duties on Users of Consumer Reports – I

- The User must have reasonable policies and procedures in place to form a reasonable belief that the report relates to the consumer about whom it was requested

- Examples of forming a reasonable belief:
 - Comparing information in the consumer report to information the user (1) maintains in its records, (2) obtains from third-parties, or (3) obtained to comply with Customer Identification Program rules
 - Verifying information in the consumer report with the consumer

Duties on Users of Consumer Reports – II

The User must have reasonable policies and procedures for furnishing a confirmed address to the NCRA if

- User can form a reasonable belief the report relates to the consumer in the User's files
- User establishes a continuing relationship with the consumer
- User regularly furnishes information to the NCRA

RESOURCES

16 C.F.R. 681 – Text of the Rules
72 Fed. Reg. No. 217 (Nov. 9, 2007) p. 63718 – Text of
Rules and Explanatory Material
www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf
– Online Federal Register Text and Explanatory
Materials
RedFlags@ftc.gov

Jonathan L. Kessler
Federal Trade Commission
1111 Superior Ave., Suite 200
Cleveland, Ohio 44114
216-263-3436
jkessler@ftc.gov
