

Mortgage Bankers Association Legal Issues and  
Regulatory Compliance Conference, Coronado,  
California May 2-5, 2010

# **FCRA/FACTA and Other Hot Legal and Regulatory Compliance Issues**

## **FACTA Anti-Identity Theft Provisions**

Jed Mayk

Stevens & Lee

Phone: 215.751.2862

email: [jema@stevenslee.com](mailto:jema@stevenslee.com)

# Topics Covered

- Fraud and Active Duty Alerts
- Blocking of Information Resulting from Identity Theft
- Business Transaction Records Relating to Identity Theft
- Disposal Rule
- Address Discrepancy Rule
- Identity Theft Prevention Programs

## Legal Authority

- Added to FCRA by the Fair and Accurate Credit Transactions Act of 2003. Codified at 15 U.S.C. § 1681c-1
- No implementing regulations. Provisions were effective on December 1, 2004. See 69 Fed. Reg. 6526 (Feb. 11, 2004)

## Purpose

- Allows consumers to notify a CRA that they may be or may become a victim of fraud or identity theft so that an alert can be placed on their file (initial and extended alerts permitted)
- Allows active duty military consumers to notify a CRA that they are on active duty so that a notation of same can be placed on their file
- Imposes rules on users of consumer reports before credit can be extended

## Potential Liability

- Private right of action for negligent and willful violations. See 15 U.S.C. §§ 1681n & 1681o
  - Negligent: actual damages, plus attorneys fees
  - Willful: actual damages or statutory damages of up to \$1,000 per violation, punitive damages and attorneys fees
- Federal and state administrative enforcement. See 15 U.S.C. § 1681s
- But, states cannot regulate in this area. See 15 U.S.C. § 1681t(b)(5)

## Who is Covered?

- A user of a consumer report that intends to extend credit to the consumer

## Limitations on Credit Extensions

- A user of a consumer report that contains a fraud or active duty alert may not extend credit (or increase a credit limit) unless it first utilizes “reasonable policies and procedures” to form a reasonable belief that it knows identity of person requesting the credit
- For initial fraud alerts and active duty alerts, the consumer **may** provide a phone number to be contacted for verification purposes
- For extended fraud alerts, consumer **must** provide a phone number or other reasonable contact method
- 15 U.S.C. § 1681c-1(h)

## Legal Authority

- Added to FCRA by the Fair and Accurate Credit Transactions Act of 2003. Codified at 15 U.S.C. §§ 1681c-2, 1681m(f), 1681m(g), and 1681s-2(a)(6)
- No implementing regulations. Provisions were effective on December 1, 2004. See 69 Fed. Reg. 6526 (Feb. 11, 2004)

## Purpose

- Restrict furnisher from refurnishing information resulting from identity theft when it receives a Section 605B blocking notice from a CRA or a consumer directly notifies furnisher that information is the result of identity theft
- Prohibit sale or placement of debt for collection that may be result of identity theft
- Require debt collectors to notify creditor when collector receives notice that debt may be fraudulent or the result of identity theft

## Potential Liability

- No private right of action under FCRA. See 15 U.S.C. §§ 1681m(h)(8) & 1681s-2(c)
- But, risk of federal and state administrative enforcement
- States cannot regulate in this area. See 15 U.S.C. § 1681t(b)(5)

## Who is Covered?

- Furnishers of information to CRAs
- Debt holders
- Debt collectors

## Receipt of Blocking Notice from CRA

- Section 1681c-2 (aka Section 605B) requires CRAs to have a process in place to block the reporting of any information in a consumer's file that the consumer claims is the result of identity theft
- Consumer must provide CRA with appropriate proof of identity, as well as an "identity theft report" (see 16 C.F.R. § 603.3(a) for detailed definition)

## Receipt of Blocking Notice from CRA (cont'd)

- CRA must then notify furnisher of the block, including the effective dates of the block. See 15 U.S.C. § 1681c-2(b)
- Furnisher must have “reasonable procedures” in place to respond to a Section 605B blocking notice in order to prevent the refurnishing of the blocked information. See 15 U.S.C. § 1681s-2(a)(6)(A)

## Receipt of Blocking Request from Consumer

- Section 1681s-2(a)(6)(B) permits the consumer to submit an identity theft report directly to the furnisher in order to prevent the information from being furnished to a CRA
- The furnisher may not furnish the disputed information to a CRA until the furnisher determines or is notified by the consumer that the information is correct

## Prohibition on Sale/Transfer of ID Theft Debt

- A holder of a debt that receives a Section 605B blocking notice may not sell the debt or place it for collection. See 15 U.S.C. § 1681m(f)
- Exceptions:
  - A debt repurchase triggered by existence of identity theft
  - The securitization or pledge of the debt as collateral
  - The transfer of the debt as the result of a merger or acquisition

## Debt Collection

- If a “debt collector” (including a servicer that has obtained a defaulted debt) learns that any information relating to a debt may be fraudulent or the result of identity theft, the collector must:
  - Notify the creditor; and
  - Upon the consumer’s request, provide the consumer with information relating to the debt
- See 15 U.S.C. § 1681m(g)

## Legal Authority

- Added to FCRA by the Fair and Accurate Credit Transactions Act of 2003. Codified at 15 U.S.C. § 1681g(e)
- No implementing regulations. Provisions were effective in mid-2004. See 15 U.S.C. § 1681g(e)(12)

## Purpose

- Provide victims of identity theft and law enforcement officials with transaction records that may help document fraudulent transactions within 30 days of receipt of a proper request

## Potential Liability

- No private right of action under FCRA. See 15 U.S.C. § 1681g(e)(6)
- But, risk of federal and state administrative enforcement.
- States cannot regulate in this area. See 15 U.S.C. § 1681t(b)(1)(G)

## Who is Covered?

- Any business entity that has provided credit, goods or services to, accepted payment from, or otherwise entered into a transaction with someone who is believed to have made unauthorized use of someone else's identity. 15 U.S.C. § 1681g(e)(1)

## What is Covered?

- Any application and business transaction records in the control of the business entity, whether maintained by the business or by another person on behalf of the business, that evidence any transaction alleged to be the result of identity theft. 15 U.S.C. § 1681g(e)(1)
- But, Section 1681g(e) does not impose any requirement to retain records that are not otherwise required to be retained in the ordinary course of business or applicable law. 15 U.S.C. § 1681g(e)(8)

## What is Covered? (cont'd)

- Nor does Section 1681g(e) permit disclosure if it is otherwise prohibited by state or federal law (but GLBA privacy rules cannot be used to withhold records from victim). 15 U.S.C. § 1681g(e)(9)
- Immunity for disclosures made in good faith. 15 U.S.C. § 1681g(e)(7)

## To Whom Must Records Be Provided?

- The identity theft victim (i.e., the consumer whose means of identification or financial information has been used or transferred without authority with the intent to commit identity theft or a similar crime)
- Any federal, state or local law enforcement agency specified by the victim
- Any law enforcement agency investigating the identity theft and authorized by the victim to take receipt of the records
- 15 U.S.C. § 1681g(e)(1)

## Procedures for Providing Records

- Unless the business has a high degree of confidence that it knows the identity of the victim making the request, the victim must provide either:
  - Government-issued ID card;
  - Personally identifying information of the same type as provided to the business by the unauthorized person; or
  - Personally identifying information that the business typically request for new applicants or for new transactions

## Procedures for Providing Records

- The victim must also provide, at the business's election, proof of the claim of identity theft in the form of:
  - A copy of a police report evidencing the identity theft claim; and
  - A properly completed FTC form of Identity theft Affidavit or another affidavit of fact that is acceptable to the business
- 15 U.S.C. § 1681g(e)(2)

## Form of Request

- In writing
- Mailed to an address specified by the business
- Business may request relevant information about the transaction (e.g., date, account number, etc.)
- Information must be provided to the victim and law enforcement free of charge
- 15 U.S.C. § 1681g(e)(3)

## When Can a Business Refuse to Provide Records?

- Disclosure would be prohibited by another state or federal law (but GLBA privacy rules cannot be used to withhold information from victim)
- After reviewing the information provided by the consumer, the business does not have a high degree of confidence that it knows the consumer's true identity
- The request for information is based on a material misrepresentation of fact; or
- The information requested is internet navigational data or similar information about a person's visit to a website or online service
- 15 U.S.C. § 1681g(e)(5), (9)

## Legal Authority

- Added to FCRA by the Fair and Accurate Credit Transactions Act of 2003. Codified at 15 U.S.C. § 1681w
- FTC, SEC, NCUA and federal banking agencies each published implementing regulations. See, e.g., 16 C.F.R. Part 682 (FTC version)

## Purpose

- Provide rules to help ensure that any person who maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose properly disposes of the information
- But, does not impose any requirement to destroy customer information, and does not alter any existing record retention requirements. See 16 C.F.R. § 682.4

## Potential Liability

- Private right of action for negligent and willful violations. See 15 U.S.C. §§ 1681n & 1681o
  - Negligent: actual damages, plus attorneys fees
  - Willful: actual damages or statutory damages of up to \$1,000 per violation, punitive damages and attorneys fees
- Federal and state administrative enforcement. See 15 U.S.C. § 1681s
- But, states cannot regulate in this area. See 15 U.S.C. § 1681t(b)(5)

## Enforcement Examples

- December, 2007 \$50,000 settlement between FTC and mortgage company that disposed of sensitive customer information in dumpsters. Company also required to undergo an information security audit every two years for the next 10 years
- December, 2009 \$35,000 settlement between FTC and mortgage company that disposed of sensitive customer information in dumpsters. Company also required to undergo an information security audit every year for the next 10 years

## Who is Covered?

- Any individual, corporation, or other entity that uses or possesses consumer information for a business purpose
- FTC has jurisdiction over the vast majority of individuals and entities subject to the Disposal Rule

## What is Covered?

- ***Consumer Information***
- Defined as any record about an individual that is a consumer report or derived from a consumer report, and also includes any compilation of such records
- But, consumer information does not include information that does not identify individuals, such as aggregate information or blind data
  - See 16 C.F.R. § 682.1(b)

## What is Covered? (cont'd)

- ***Consumer report***
  - The communication of any information by a consumer reporting agency that bears on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected to serve as a factor in establishing a consumer's eligibility for credit, insurance, employment purposes, or any other permissible purpose under FCRA. See 15 U.S.C. § 1681a(d)

## What is Covered (cont'd)

- Consumer reports obtained from consumer reporting agencies are covered
- Also covered are any records that are derived from a consumer report (e.g., underwriting sheets, employment records, tenant applications that contain information from a consumer report)
- See, e.g., 12 C.F.R. Part 30, Appendix B (additional examples of consumer information)

## Proper Disposal

- Standard is ***reasonable measures*** to protect against unauthorized access to or use of consumer information in connection with its disposal. See 16 C.F.R. § 682.3(a)
- Can incorporate disposal procedures into the required GLBA information security program
- Examples of reasonable measures include:
  - Policies and procedures that require the burning, pulverizing, or shredding of papers containing consumer information
  - Policies and procedures that require the destruction or erasure of electronic media containing consumer information

## Proper Disposal (cont'd)

- Due diligence on disposal vendors:
  - Review an independent audit of the disposal company's operations
  - Obtain information about the disposal company from references
  - Require the disposal company to be certified by a recognized trade association or similar third party
  - Review and evaluate the disposal company's information security policies and procedures
  - Take other appropriate measures to determine the competency and integrity of the disposal company

## Legal Authority

- Added to FCRA by the Fair and Accurate Credit Transactions Act of 2003. Codified at 15 U.S.C. § 1681c(h)(2)
- Joint regulations published by FTC, NCUA and federal banking agencies had a mandatory compliance date of November 1, 2008. See, e.g., 16 C.F.R. Part 641 (FTC version)

# Address Discrepancy Rule

## Purpose

- Ensure that users of consumer reports have reasonable policies and procedures in place to react to a notice of address discrepancy from a nationwide consumer reporting agency

## Potential Liability

- Private right of action for negligent and willful violations. See 15 U.S.C. §§ 1681n & 168o
  - Negligent: actual damages, plus attorneys fees
  - Willful: actual damages or statutory damages of up to \$1,000 per violation, punitive damages and attorneys fees
- Federal and state administrative enforcement. See 15 U.S.C. § 1681s
- Can states regulate in this area? Do requirements “relat[e] to information contained in consumer reports”? See 15 U.S.C. § 1681t(b)(1)(E)

# Address Discrepancy Rule

## Who is Covered?

- Any user of a consumer report

# Address Discrepancy Rule

## Background

- Since December 1, 2004, nationwide consumer reporting agencies have been required to notify users of consumer reports when there is a substantial difference between the consumer's address identified by the user in its request for a consumer report and the address information in the consumer reporting agency's file. See 15 U.S.C. § 1681c(h)(1)
- The regulations now provide guidance on what a user must do when it receives an address discrepancy notice. See 16 C.F.R. § 641.1

# Address Discrepancy Rule

## Verifying the Consumer's Identity

- Policies and procedures to allow user to form a ***reasonable belief*** that consumer report relates to consumer about whom report was requested
  - Applies regardless of whether an account is ever opened
  - Applies even after an account is opened

## Verifying the Consumer's Identity (cont'd)

- Acceptable policies and procedures include the customer identification procedures under the USA PATRIOT Act (e.g., collect name, address, date of birth and social number and verify by documentary methods). See 31 C.F.R. § 103.121
- Can also verify information in the consumer report with the customer

## Verifying the Consumer's Identity (cont'd)

- If identity cannot be adequately verified, the user should not use the consumer report
- Could also trigger other obligations (e.g., SAR filing for certain institutions, implementing identity theft **red flag** procedures, etc.)

## Reporting a Confirmed Address

- Policies and procedures must also be in place to provide to the consumer reporting agency an address that the user has reasonably confirmed is accurate if three conditions are met:
  - The user can form a reasonable belief that report relates to consumer about whom report was requested

## Reporting a Confirmed Address (cont'd)

- The user establishes a continuing relationship with the consumer – i.e., does not apply to notices received in course of existing relationships (but note: users still have FCRA obligations to update information on existing customers); and
- The user regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy was obtained

## Reporting a Confirmed Address (cont'd)

- Accuracy of address may be confirmed by:
  - Verifying with the consumer;
  - Reviewing your own records;
  - Using third party sources; or
  - Other reasonable means
- Confirmed address must be provided as part of information regularly furnished for the ***reporting period in which the relationship is established***

## Legal Authority

- Added to FCRA by the Fair and Accurate Credit Transactions Act of 2003. Codified at 15 U.S.C. § 1681m(e)
- Joint regulations published by FTC, NCUA and federal banking agencies had a mandatory compliance date of November 1, 2008. See, e.g., 16 C.F.R. Part 681 (FTC version)
- But, FTC has deferred enforcement as to entities under its jurisdiction until June 1, 2010

## Purpose

- Address and mitigate the risk of identity theft for customers of financial institutions and creditors

## Potential Liability

- No private right of action under FCRA. See 15 U.S.C. §§ 1681m(h)(8) & 1681s-2(c)(3)
- But, risk of federal and state administrative enforcement. See 15 U.S.C. §§ 1681s & 1681s-2(d)
- States cannot regulate in this area. See 15 U.S.C. § 1681t(b)(5)

## “Identity Theft”

- A fraud committed or attempted using the ***identifying information*** of another person without authority
- ***Identifying information*** – any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any

## “Identity Theft” (cont’d)

- Name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
- Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

## “Identity Theft” (cont’d)

- Unique electronic identification number, address, or routing code; or
- Telecommunications identifying information or access device (as defined in 18 U.S.C. 1029(e))
- See 16 C.F.R. § 603.2

## Who is Covered?

- **Financial institutions** – Banks, thrifts, credit unions and other holders of transaction accounts. See 15 U.S.C. §1681a(t)
- **Creditors** – defined by reference to the federal Equal Credit Opportunity Act. See 15 U.S.C. § 1601a
  - Someone who regularly lends money or sells goods or services and accepts payment on a deferred basis. See 15 U.S.C. § 202.2(j),(l)
  - Can also include credit arrangers (e.g., brokers and debt collectors in some cases)

## Who is Covered? (cont'd)

- ***Account***

- A continuing relationship established by an individual, corporation, partnership, trust, etc.;
- with a financial institution or creditor;
- in order to obtain a product or service;
- for personal, family household **or** business purposes
- Examples include: a loan account, purchase on a deferred payment basis, or deposit account
- See 16 C.F.R. § 681.1(b)(1)

## Who is Covered? (cont'd)

### **Covered Account**

- An account primarily for personal, family or household purposes that is designed to permit multiple payments or transactions (e.g., credit card account, auto loan, margin account, checking account, cell phone or utility account);
- **OR**
- Any other account for which there is a reasonably foreseeable risk to customers or safety and soundness from identity theft (e.g., small business accounts)
- See 16 C.F.R. § 681.1(b)(3)

## Requirement

- If you are a financial institution or creditor that offers covered accounts, then you must have a **written** Identity Theft Prevention Program (“ITPP”)
  - Must be designed to detect, prevent **and** mitigate identify theft at account opening and for any existing covered account;
  - Must be appropriate to size and complexity of institution/creditor and nature of activities
    - See 16 C.F.R. § 681.1(d)(1)

## Elements

- The ITPP must contain policies and procedures to:
  - Identify and incorporate applicable identity theft **Red Flags** from the interagency Red Flag guidelines, applicable supervisory guidance, incidents of identity theft that the institution or creditor has experience, and methods of identity theft that the institution or creditor has identified that reflect changes in identity theft risks;
  - Detect Red Flags that have been incorporated into the ITPP;
  - Design appropriate responses to Red Flags that are detected; and
  - Ensure that the ITPP is updated periodically

## Administration

- Initial ITPP must be approved by the Board of Directors or an appropriate Board committee
- Board, committee or senior management-level employee must be involved in oversight, development, implementation and administration (including receipt of an annual report on compliance, effectiveness, significant changes to the ITPP, significant identity theft incidents, etc.);
- Staff training; and
- Appropriate oversight of service providers