



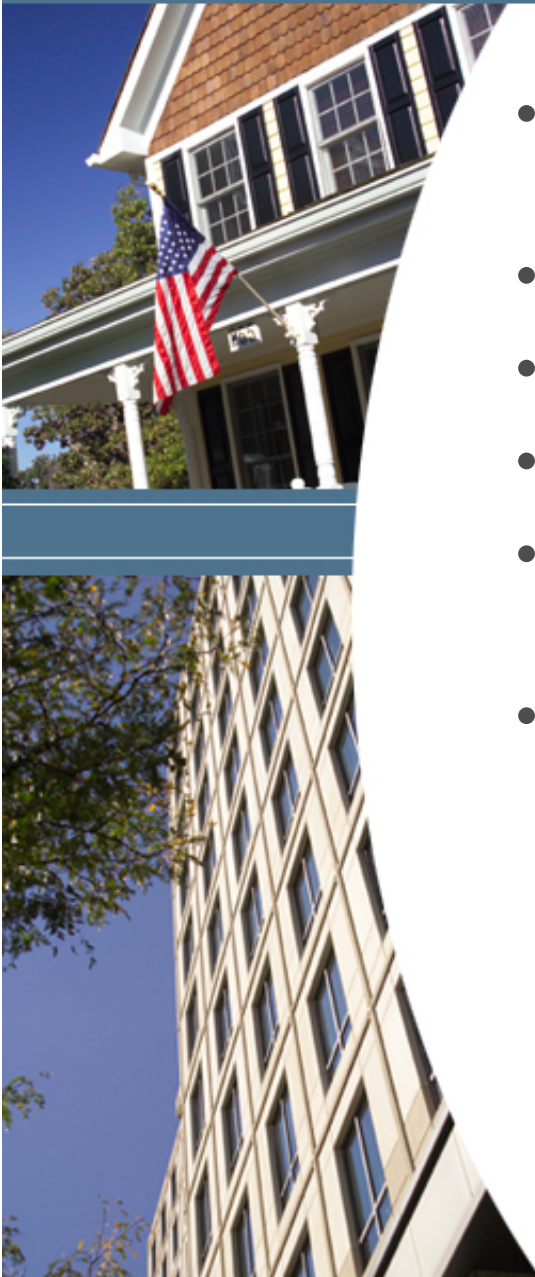
FCRA, FACT Act and Data Security

Andrew Smith

Morrison & Foerster LLP

Washington, DC

Overview



- Final Red Flags Rule
 - » Commercial application
- Final Affiliate Marketing Rule
- Proposed Furnisher Rule and Direct Dispute Rule
- Risk-Based Pricing Rule
- Data Security
 - » Private, State and Federal enforcement
- Firm Offer Litigation Update

Final Red Flags Rule (FACT Act)



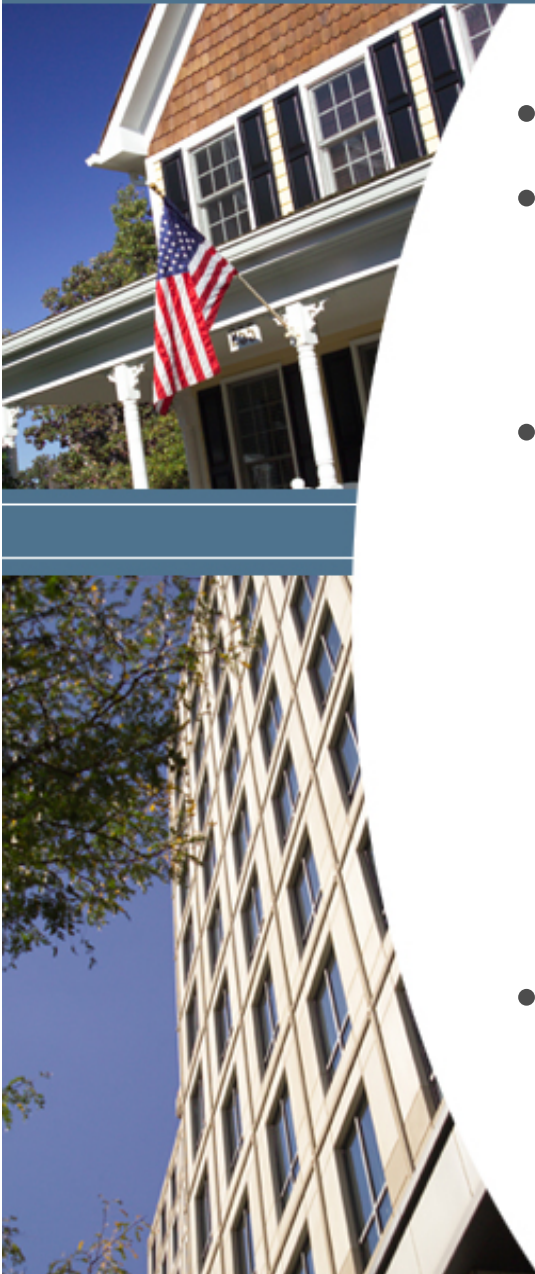
- Three parts:
 - » Rule – 16 CFR 681.2
 - » Guidelines – 16 CFR pt. 681, App. A
 - » Red Flags – 16 CFR pt. 681, App. A, Supp. A
- **Rule:** Creditors and depository institutions must
 - (1) Assess whether they offer “covered accounts”
 - Consumer accounts involving multiple payments or transactions
 - Commercial loans, if there is a “reasonably foreseeable risk” to customers or to safety and soundness from identity theft
 - › Consider methods of account opening and access; prior experiences with ID theft
 - (2) Develop *written* ID theft prevention program
 - Board approval, annual staff reports and updates

Final Red Flags Rule (FACT Act)



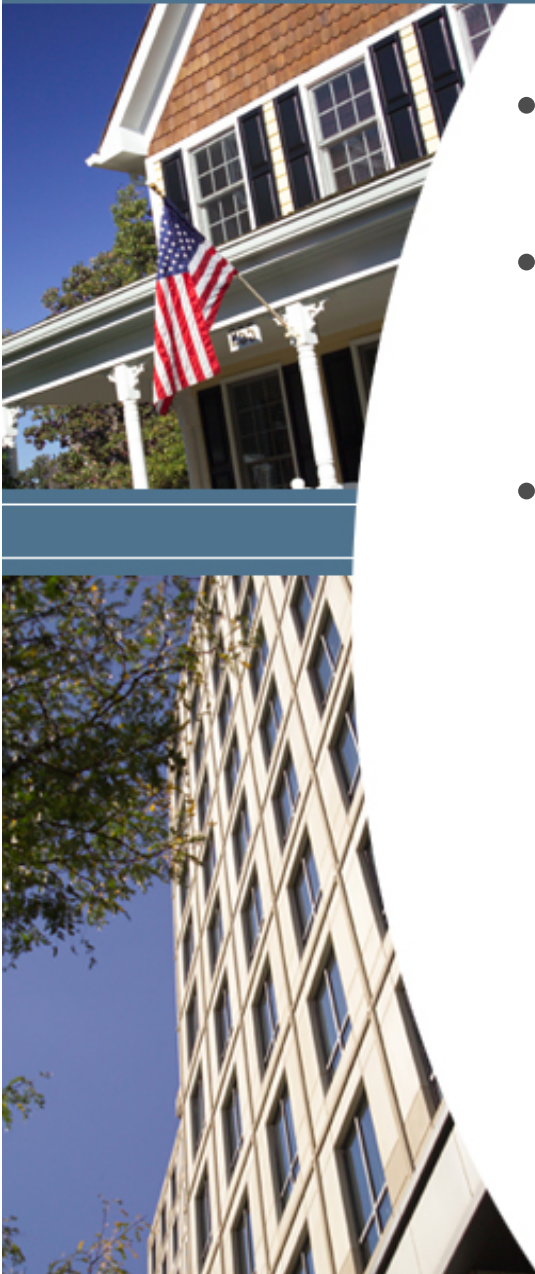
- **Guidelines:** considered when developing program to
 - » **Identify** relevant red flags
 - » **Detect** those red flags
 - » **Respond** when red flags are detected
- **Red Flags:** possible indicators of ID theft
- Mandatory compliance date: Nov. 1, 2008
 - » Preempts state law requirements
- Administratively enforced
 - » No private right of action

Final Affiliate Marketing Rule (FACT Act)



- Compliance required by Oct. 1, 2008
- May not use “eligibility information” received from an affiliate for marketing
 - » Unless consumer is given notice and opt-out
- Notice may not be necessary:
 - » Pre-existing business relationship
 - Loan within 18 months; inquiry within 3 months
 - » Inquiry or authorization
 - » “Constructive sharing”
 - » Information received in a common database before Oct. 1, 2008
 - » Aggregated or blind data
- Private Right of Action

Furnisher and Direct Dispute Rules (FACT Act)



- Guidelines and regulations for furnishers regarding the accuracy and integrity of information
- Regulations that identify when a furnisher is required to reinvestigate a dispute received directly from a consumer
- Proposed Dec. 2007
 - » Comments were due Feb. 11, 2008

Risk-Based Pricing Rule (FACT Act)



- Joint FRB/FTC rule
- General requirement: risk-based pricing notice when you
 - » Based on a consumer report,
 - » Provide the consumer with credit “on material terms that are
 - materially less favorable than
 - the most favorable terms
 - available to a substantial proportion of consumers
 - from or through” the lender
- Rule must address exceptions
 - » where a risk-based pricing notice “would not significantly benefit consumers”
- Agencies may propose a general rule, with alternatives for different types of transactions

Data Security: Private Actions



- Class actions following a data breach largely unsuccessful
- No compensable injury under state common law (negligence)
 - » *Pisciotta v. Old Nat'l Bancorp* (7th Cir. 2007). Present and future identity theft-monitoring costs are not compensable damages
 - » *But see Stollenwerk v. Tri-West* (9th Cir. 2007). Affirmed dismissal as to plaintiffs who merely purchased credit monitoring, but not as to plaintiff who alleged actual identity theft, although vaguely
- No Article III standing
 - » Increased risk of ID theft is not cognizable harm
 - » *Bell v. Acxiom* (E.D. Ark. 2006); *Key v. DSW* (S.D. Ohio 2006); *Giordano v. Wachovia* (D.N.J. 2006)

Data Security: State Enforcement



- Texas AG
 - » 2005 Identity Theft Enforcement and Protection Act
 - Tex. Bus. & Com. Code Ann § 48.102
 - » CVS, Radio Shack, others: dumpster cases
 - » CVS settlement: injunction + \$315,000
- Connecticut AG
 - » Pfizer: investigation into breach of employee data
 - Employee loaded unauthorized file sharing software onto a company laptop
 - » Accenture: contract action
 - Data tape containing CT state data stolen from car in Ohio

Data Security: State Enforcement



- New York AG
 - » CS STARS LLC (Claims administration unit of Marsh, Inc.)
 - » Lost hard drive containing data on 540,000 workers' comp claimants
 - Noticed computer was missing: May 9, 2006
 - Notified law enforcement: June 29 (7 weeks later)
 - 540,000 consumer notices sent: July 18
 - Computer recovered: July 26
 - Investigation showed data had not been accessed
 - » Settlement
 - 7 week delay = violation of NY security breach law
 - Assurance of Voluntary Compliance
 - \$60,000 to cover costs of investigation

Data Security: FTC Enforcement



- Unfairness
 - » TJX
 - » Reed Elsevier/Seisint
- GLBA and Deception
 - » Goal Financial (student lender)
 - » Employees sold 7,000 files to third parties without authorization
 - » Employee sold surplus hard drives that contained information about 34,000 consumers
 - » Privacy notice:
 - “We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.”
- FCRA/FACT Act Disposal Rule
 - » American United Mortgage Co.
 - » Credit report information in unsecured dumpster
 - » \$50,000 penalty

Firm Offer Litigation Update



- *Cole* applies only to product tie-ins?
 - » *Dixon v. Shamrock Financial* (1st Cir. Apr. 3, 2008)
 - » *Murray v. New Cingular* (7th Cir. Apr. 16, 2008)
 - » *Klutho v. Oxford Lending* (E.D. Mo. Apr. 9, 2008)
 - Recants earlier holdings that firm offers must have “value”
- Settlements: *Yeagley v. Wells Fargo* (N.D. Cal.)
 - » 3.8 million class members
 - » \$50 rebate on new first mortgage loan
 - » Attorney’s fees chopped from \$1.5 million to \$326,000