Privacy and Information Security Law

Randy Canis

CLASS 11

Financial Data pt. 1;
Data Security

Financial Data pt. 1

2

A. THE FAIR CREDIT REPORTING ACT

3

Credit Reports

- Why do credit reports matter?
  - Credit score affects interest rate
  - Employers use credit reports to make hiring and promotion decisions

4

Fair Credit Report Act (FCRA)

- "FCRA applies to 'any consumer reporting agency' that furnishes a 'consumer report.' 15 U.S.C. §1681b."

5

What is a Consumer Report?

- "A '**consumer report**' is any type of communication by a consumer reporting agency 'bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living.' This communication must be used or expected to be used in part to establish a **consumer's eligibility** for credit, insurance, employment, or other permissible uses of credit reports as defined in FCRA. 15 U.S.C. §1681a."

6

What is a Consumer Reporting Agency?

- "A '**consumer reporting agency**' is defined as '[a]ny person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the **practice of assembling or evaluating consumer credit information** or other information on consumers for the purpose of **furnishing consumer reports to third parties**.' § 1681b(f)."

7

FCRA Enforcement

- FTC and Consumer Financial Protection Bureau (CFPB) coordinate enforcement
- People harmed can sue under a private right of action

8

FCRA Preemption

- "**FCRA preempts state law** relatively broadly and does so by reserving a large number of subjects for federal law. … [However,] it permits states to engage in further regulation regarding the larger subject area, which is **identity theft**."

9

US v. Spokeo, Inc.

- C.D.CA 2012
- Issue
  - Is Spokeo in violation of the FCRA?

10

US v. Spokeo, Inc.

- "The consumer profiles Spokeo provides to third parties are 'consumer reports' as defined in section 603(d) of the FCRA, 15 U.S.C. §1681a(d). … Section 607(a) of the FCRA, 15 U.S.C. §1681e(a), requires that every consumer reporting agency maintain reasonable procedures to **limit the furnishing of consumer reports** for enumerated 'permissible purposes.' These reasonable procedures include making reasonable efforts to **verify the identity** of each prospective user of consumer report information and the **uses certified by each prospective user** prior to furnishing such user with a consumer report. … Spokeo has failed to maintain such reasonable procedures."

11

Spokeo, Inc. v. Robins

- Supreme Court 2016
- Issue
  - Does Robins have standing to maintain a federal court action against petitioner Spokeo under the FCRA?
- Case history
  - DC dismissed for lack of standing
  - 9th Circuit reversed

12

Spokeo, Inc. v. Robins

- Background
  - "Spokeo operates a 'people search engine.' If an individual visits Spokeo's Web site and inputs a person's name, a phone number, or an e-mail address, Spokeo conducts a computerized search in a wide variety of databases and provides information about the subject of the search. Spokeo performed such a search for information about Robins, and some of the information it gathered and then disseminated was incorrect. When Robins learned of these inaccuracies, he filed a complaint on his own behalf and on behalf of a class of similarly situated individuals."

13

Spokeo, Inc. v. Robins

- "[T]he [FCRA] regulates the creation and the use of 'consumer report[s]' [] by 'consumer reporting agenc[ies]' [] for certain specified purposes, including credit transactions, insurance, licensing, consumer-initiated business transactions, and employment."

14

Spokeo, Inc. v. Robins

- "The FCRA imposes a host of requirements concerning the creation and use of consumer reports. As relevant here, the Act requires consumer reporting agencies to '**follow reasonable procedures to assure maximum possible accuracy** of' consumer reports, §1681e(b); to **notify** providers and users of consumer information of their **responsibilities under the Act**, §1681e(d); to **limit the circumstances** in which such agencies provide consumer reports '**for employment purposes**,' §1681b(b)(1); and to post **toll-free numbers** for consumers to request reports, §1681j(a)."

15

Spokeo, Inc. v. Robins

- Liability to an individual for willful failure to comply
  - Actual damages, or
  - Statutory damages of $100 to $1,000 per violation, costs of the action and attorney's fees, and possibly punitive damages.

16

Spokeo, Inc. v. Robins

- Case further considers whether Robins has sufficient standing to bring a cause of action by sufficiently alleging an injury
- Case sent back to 9th Circuit for further consideration

17

Permissible Uses of Consumer Reports

- "Pursuant to 15 U.S.C. §1681b, a consumer reporting agency can furnish a consumer report only under certain circumstances or for certain uses:
- (1) in response to a court order or grand jury subpoena;
- (2) to the person to whom the report pertains;
- (3) to a 'person which [the agency] has reason to believe' intends to use the information in connection with (a) the extension of credit to a consumer; (b) employment purposes; (c) insurance underwriting; (d) licensing or the conferral of government benefits; (e) assessment of credit risks associated with an existing credit obligation; (f) 'legitimate business need' when engaging in 'a business transaction involving the consumer';
- (4) to establish a person's capacity to pay child support."

18

Private Right of Action

- "[A] private right of action for "any consumer" regarding "[a]ny person" who under false pretenses gains a consumer report, or who willfully or knowingly fails to comply with certain of its requirements. §1681n(a). It also provides for punitive damages, reasonable attorney's fees, and statutory damages of $1,000 or actual damages."

19

Employment Purposes

- Employer or potential employer must disclose in writing that a consumer report may be obtained, and consumer must authorize in writing
- Person seeking report must certify the report is obtained with consent and will not use the report in violation of the law
- If the person obtaining the report takes an adverse action, the person must provide the consumer with a copy of the report and a description of the rights of the consumer under the FCRA

20

Investigative Consumer Reports

- "An '**investigative consumer report**' is 'a consumer report or portion thereof in which information on a **consumer's character**, general reputation, personal characteristics, or mode of living is obtained through personal interviews, with neighbors, friends, or associates.' §1681a(f)."

21

Limited Set of "Permissible Purposes"

- "The FCRA identifies a **limited set of "permissible purposes" for obtaining and using a consumer report**. See 15 U.S.C. §1681b(a)(3); see also 15 U.S.C. §1681b(f). Those permissible purposes provide that a person may only access a consumer report if he:
- (A) intends to use the information in connection with a **credit transaction involving the consumer** on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; or
- (B) intends to use the information for **employment purposes**; or
- (C) intends to use the information in connection with the **underwriting of insurance** involving the consumer; or

22

Limited Set of "Permissible Purposes"

- (D) intends to use the information in connection with a determination of the consumer's **eligibility for a license** or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status; or
- (E) intends to use the information, as a **potential investor** or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation; or
- (F) otherwise has **a legitimate business need** for the information—
  - (i) in connection with a business transaction that is initiated by the consumer; or
  - (ii) to review an account to determine whether the consumer continues to meet the terms of the account.
- 15 U.S.C. §1681b(a)(3)."

Smith v. Bob Smith Chevrolet, Inc.

23

Legitimate Business Need

- "[N]early every federal court addressing this issue has similarly held that the "**legitimate business need**" permissible purpose should be **narrowly construed** in the context of the other five enumerated purposes …"
- Smith v. Bob Smith Chevrolet, Inc.

24

Consumer Rights and Agency Responsibilities

- Agency must follow reasonable procedures to assure maximum accuracy

25

Disclosure to the Consumer

- The FCRA requires that consumer reporting agencies, upon request of the consumer, disclose, among other things:

1) All information in the consumer's file at the time of the request, except . . . any information concerning credit scores or any other risk scores or predictors relating to the consumer.
2) The sources of the information. . . .
3) Identification of each person . . . that procured a consumer report [within two years for employment purposes; within one year for all other purposes] . . . .
4) The dates, original payees, and amounts of any checks upon which is based any adverse characterization of the consumer, included in the file at the time of disclosure. … §1681g.

26

Consumer Accuracy Issues

- If inaccurate, incomplete, or cannot be verified, the agency must promptly delete it.

27

Civil Liability and Qualified Immunity

28

Civil Liability

- "[A]ny person who 'willfully fails to comply with any requirement' of the FCRA is liable to the consumer for actual damages or statutory damages between $100 and $1,000, as well as punitive damages and attorneys' fees and costs. §1681n."

29

Qualified Immunity and Statute of Limitations

- FCRA provides qualified immunity to credit reporting agencies
- "Plaintiffs can only state tort actions when 'defendants acted with malice or willful intent to injure plaintiff.' §1681h."

30

Sarver v. Experian Information Solutions

- 7th Cir. 2004
- Issue
  - Damages available for a possible violation of FCRA

31

Sarver v. Experian Information Solutions

- Inaccurate bankruptcy notation in P's credit report
- P wrote Experian to information of error and asked for removal
- Experian asked for further identifying information
- P did not provide the requested information and filed a lawsuit

32

Sarver v. Experian Information Solutions

- "Section 1681i requires a **credit reporting agency to reinvestigate** items on a credit report when a consumer disputes the validity of those items. An agency can terminate a reinvestigation if it determines the complaint is frivolous, 'including by reason of a failure by a consumer to provide sufficient information to investigate the disputed information.' §1681i(a)(3)."

33

Sarver v. Experian Information Solutions

- "In order to prevail on his claims, Sarver must show that he suffered damages as a result of the inaccurate information."
- "Experian must be notified of an error before it is required to reinvestigate."

34

Sarver v. Experian Information Solutions

- "A credit reporting agency is **not liable** under the FCRA if it followed '**reasonable procedures** to assure maximum possible accuracy,' but nonetheless reported inaccurate information in the consumer's credit report."

35

Identity Theft and Consumer Reporting

36

One-Call Fraud Alerts

- Consumers need only contact once consumer reporting agency of potential fraud
- The agency receiving the notification must notify the other consumer reporting agencies

37

Business Transaction Data

- Victim's have a right to disclosure information regarding fraudulent transactions
- Victim must properly identify himself/herself and make the request in writing

38

Private Cause of Action

- "The FCRA provides a private cause of action for those damaged by violations of the statute. *See* 15 U.S.C.A. §§1681n, 1681o. A successful plaintiff can recover both **actual and punitive damages** for willful violations of the FCRA, *id.* §1681n(a), and actual damages for negligent violations, *id.* §1681o(a). **Actual damages may include not only economic damages, but also damages for humiliation and mental distress**. The statute also provides that a successful plaintiff suing under the FCRA may recover **reasonable attorney's fees**. 15 U.S.C.A. §§1681n(a)(3), 1681o(a)(2). …"
- Sloane v. Equifax Information Services, LLC

39

Data Security

40

A. INTRODUCTION

41

Victims of Data Breaches

- Verizon Data Breach Investigations Report 2013

42

B. DATA SECURITY BREACH NOTIFICATION STATUTES

43

CA Data Breach Statute

- "Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall **disclose any breach** of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in **the most expedient time possible and without unreasonable delay**, consistent with the legitimate needs of law enforcement."

44

States/Federal Government Data Breach Laws

- 47 States and D.C. with breach notification laws
  - Need to understand the differences so that the business can comply with the notification requirements

45

Breach Law Variations

1) the definition of covered information;
2) the trigger for notification;
3) any exceptions to the law's notification requirement;
4) a requirement of notification to a state agency or attorney general;
5) the presence or absence of a substantive requirement for data security; and
6) the presence or absence of a private right of action.

46

Covered Information

- Notice-triggering information (for CA + FL & GA)
- "[F]irst name or initial and last name" and any of the following list of other data: Social Security number; driver's license number; financial account number plus a password."
- Since 2013 includes "user names or e-mail addresses in combination with a password or a security question and answer that would permit access to an online account."

47

Trigger for Notification

- "[S]tates generally require notification whenever there is a reasonable likelihood that an unauthorized party has 'acquired' person information. A minority of states have adopted a higher standard. These states consider whether there is a reasonable likelihood of 'misuse' of the information, or 'material risk' of harm to the person. The idea is that a breach letter should not be sent to the affected public unless there is a more significant likelihood of harm."

48

Notification to State Agency or Attorney General

- "All the breach notification statutes require notification to the **affected party**. …States that **require notice to a state agency or attorney general** include Alaska, California, Connecticut, Florida, Hawaii, Illinois, Indiana, Iowa, Maryland, Massachusetts, New York, North Carolina, South Carolina, Vermont, and Virginia."

49

Substantive Data Security

- Some states create a substantive duty to take reasonable steps to safeguard data.
- While generally open-ended, the duties generally related to requiring reasonableness in measures taken

50

Private Right of Action

- Only in a minority of states
- Through a separate statute or under the state's unfair or deceptive trade practices act.

51

C. CIVIL LIABILITY AND STANDING

52

Pisciotta v. Old National Bancorp

- 7th Cir. 2007
- Issue
  - Does ONB owe its users compensation when a hacker used confidential information of its users?
- History
  - S.D.IN – no
  - 7th Cir. – affirm

53

Pisciotta v. Old National Bancorp

- NCR is a hosting facility that maintained the ONB website had a security breach and notified ONB
- ONB notified its customers of the security breach

54

Pisciotta v. Old National Bancorp

- P do not allege direct financial loss or being the victim of an identity theft
- "The plaintiffs requested '[c]ompensation for all economic and emotional damages suffered as a result of the Defendants' acts which were negligent, in breach of implied contract or in breach of contract,' and '[a]ny and all other legal and/or equitable relief to which Plaintiffs . . . are entitled, including **establishing an economic monitoring procedure** to insure [sic] prompt notice to Plaintiffs . . . of any attempt to use their confidential personal information stolen from the Defendants.'"

55

Pisciotta v. Old National Bancorp

- "As many of our sister circuits have noted, the injury-in-fact requirement **can be satisfied** by a threat of future harm or by an act which harms the plaintiff only by **increasing the risk of future harm that the plaintiff would have otherwise faced**, absent the defendant's actions. We concur in this view."

56

Pisciotta v. Old National Bancorp

- "The provisions of the statute applicable to private entities storing personal information **require only that a database owner *disclose* a security breach to potentially affected consumers**; they do not require the database owner to take any other affirmative act in the wake of a breach. If the database owner fails to comply with the only affirmative duty imposed by the statute — the duty to disclose — the statute provides for enforcement *only* by the Attorney General of Indiana. It creates **no private right of action** against the database owner by an affected customer. It imposes no duty to compensate affected individuals for inconvenience or potential harm to credit that may follow. …"

57

Future Risk of Harm=Standing?

- "[A] number of courts have had occasion to decide whether the "risk of future harm" posed by data security breaches confers standing on persons whose information may have been accessed. Most courts have held that such **plaintiffs lack standing because the harm is too speculative**. … Here, no evidence suggests that the data has been—or will ever be—misused. The present test is actuality, not hypothetical speculations concerning the possibility of future injury. Appellants' allegations of an increased risk of identity theft resulting from a security breach are therefore insufficient to secure standing."
- Reilly v. Ceridian Corp. (3rd. Cir. 2011)

58

Resnick v. AvMed

- 11th Cir. 2012
- Issue
  - Liability for a data breach

59

Resnick v. AvMed

- Two laptop computers stolen from AvMed's office
- "AvMed did not take care to secure these laptops, so when they were stolen the information was readily accessible. The laptops were sold to an individual with a history of dealing in stolen property. The unencrypted laptops contained the sensitive information of approximately 1.2 million current and former AvMed members."

60

Resnick v. AvMed

- "Plaintiffs allege that they have become victims of identity theft and have suffered monetary damages as a result. This constitutes an injury in fact under the law."

61

Resnick v. AvMed

- "Generally, to prove that a data breach caused identity theft, the pleadings must include **allegations of a nexus between the two instances beyond allegations of time and sequence**. … Here, Plaintiffs allege a nexus between the two events that includes **more than a coincidence of time and sequence**: they allege that the sensitive information on the stolen laptop was the same sensitive information used to steal Plaintiffs' identity. Plaintiffs explicitly make this connection when they allege that Curry's identity was stolen by changing her address and that Moore's identity was stolen by opening an E*Trade Financial account in his name…"

62

Resnick v. AvMed

- "Plaintiffs have **sufficiently alleged a nexus** between the data theft and the identity theft and therefore meet the federal pleading standards. Because their contention that the data breach caused the identity theft is plausible under the facts pled, Plaintiffs **meet the pleading standards** for their allegations on the counts of negligence, negligence *per se,* breach of fiduciary duty, breach of contract, breach of implied contract, and breach of the implied covenant of good faith and fair dealing. …"

63

Data Breach Theories of Harm

- "(1) The exposure of their data has caused them **emotional distress**;
- (2) The exposure of their data has subjected them to an **increased risk of harm** from identity theft, fraud, or other injury; or
- (3) The exposure of their data has resulted in their having to expend time and money **to prevent future fraud**, such as signing up for credit monitoring, contacting credit reporting agencies and placing fraud alerts on their accounts, and so on."
- Arguments have generally been dismissed

64

D. FTC REGULATION

65

Enforcement Actions

- "The FTC's initial **enforcement actions for data security** involved companies that failed to live up to promises made about **data security in their privacy policies**. The FTC has deemed the failure to follow statements made in a privacy policy to be a deceptive act or practice. A deceptive act or practice is a material 'representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment.'

66

Unfair Data Security Practices

- "Under the FTC Act, a practice is unfair if it 'causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or competition.' 15 U.S.C. §45(n)."

67

Section 5

- Violation of a consent decree results in fines
- Can issue fines under other sections
- FTC can obtain injunctive relief
- No private right of action

68

FTC v. Wyndham Worldwide Corp.

- 3rd Circuit 2015
- Issue
  - Does the FTC have authority to regulate cyberspace and its Wyndham under fair notice?

69

FTC v. Wyndham Worldwide Corp.

- Wyndham
  - Hotel company
  - Operates a property management system and computer network

70

FTC v. Wyndham Worldwide Corp.

- "The FTC alleges that, at least since April 2008, Wyndham engaged in **unfair cybersecurity practices** that, 'taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft.'"

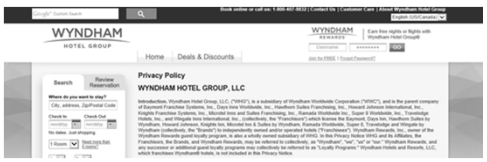
71

FTC v. Wyndham Worldwide Corp.

- What were Wyndham's failures?
  - Stored payment card info in clear text
  - Easily guessed passwords
  - Failed to use readily available security measures (e.g., firewalls)
  - Failed to take adequate precautions with company and vendor connecting computers
  - Failed to employ reasonable measures to detect and prevent unauthorized access or conduct security investigations
  - Did not follow proper incident response procedures

72

FTC v. Wyndham Worldwide Corp.



73

FTC v. Wyndham Worldwide Corp.

- Overstated privacy policy
- "The FTC alleges that, contrary to this policy, Wyndham did not use encryption, firewalls, and other commercially reasonable methods for protecting consumer data."

74

FTC v. Wyndham Worldwide Corp.

- Cybersecurity attacks
  - 3 occasions in 2008 and 2009
  - 1st LAN access through a hotel, brute force guessing IDs and passwords, accessed an admin account, obtain unencrypted consumer data on 500K accounts, information sent to Russia
  - 2nd attached through admin account; Wyndham unaware until consumer complaints over fraud charges, memory-scraping malware on computers; obtained payment card info for 50K users

75

FTC v. Wyndham Worldwide Corp.

- Cybersecurity attacks
  - 3rd attack access to property management servers allowed obtain card information for 69K users
  - Payment card info for a total of 619K consumers, 10.6 million in fraud loss, and other consumer injuries

76

FTC v. Wyndham Worldwide Corp.

- "Unfair methods of competition in commerce" was meant by Congress to be flexible and evolving
- Language evolved to "unfair methods of competition in or affecting commerce"

77

FTC v. Wyndham Worldwide Corp.

- Three Governing factors
  1) Offends public policy
  2) Immoral, unethical, oppressive, or unscrupulous,
  3) Causes substantial injury to consumers, competitors, and/or other businessmen

78

FTC v. Wyndham Worldwide Corp.

- §45(n) – "The Commission shall have no authority under this section . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless **the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits** to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination."

79

FTC v. Wyndham Worldwide Corp.

- "A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business."

80

FTC v. Wyndham Worldwide Corp.

- "For good reason, Wyndham does not argue that the cybersecurity intrusions were unforeseeable. That would be particularly implausible as to the second and third attacks."

81

FTC v. Wyndham Worldwide Corp.

- Fair Notice?
- "[W]e and our sister circuits frequently use language implying that a conviction violates due process if the defendant could not reasonably foresee that a court might adopt the new interpretation of the statute."

82

FTC v. Wyndham Worldwide Corp.

- "Subsection 45(n) asks whether 'the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.' While far from precise, this standard informs parties that the relevant inquiry here is a cost-benefit analysis, … that considers a number of relevant factors, including the **probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity**."

83

FTC v. Wyndham Worldwide Corp.

- "Fair notice is satisfied here as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute."

84

FTC v. Wyndham Worldwide Corp.

- "Wyndham's as-applied challenge falls well short given the allegations in the FTC's complaint. As the FTC points out in its brief, the complaint does not allege that Wyndham used *weak* firewalls, IP address restrictions, encryption software, and passwords. Rather, it alleges that Wyndham **failed to use *any* firewall at critical network points**, [] did **not restrict specific IP addresses *at all***, *[]* d**id not use *any* encryption for certain customer files**, *id.* [] and **did not require some users to change their default or factory-setting passwords *at all*** []. Wyndham did not respond to this argument in its reply brief."

85

In the Matter of Trendnet

- Issue
  - FTC enforcement issue with devices having a live audio and video stream viewable over the Internet with a password that enabled others to view the stream without permission

86

In the Matter of Trendnet

87

In the Matter of Trendnet

- Software flaw allows feeds to be publicly viewable
- People gained access to live feeds not intended for the public
- News stories included images from the feeds along with photos of associated locations based on address

88

In the Matter of Trendnet

- "Researchers discovered other security vulnerabilities, including the transmission of unencrypted passwords. TRENDnet also had failed to perform ordinary security testing."

89

In the Matter of Trendnet

- No more misrepresentations
- Establish and implement a comprehensive security program
- Risk assessments, risk personnel, safeguards, testing and monitoring, etc.
- Notify those affected
- 20 year order

90

Program Completed

91