NIST/OCR HIPAA SECURITY RULE CONFERENCE

Cora Tung Han
FTC, Division of Privacy and Identity Protection
June 6, 2012

Roadmap

- Background
- FTC Privacy Report
- Privacy and Data Security Enforcement
- Health Breach Notification Rule

FTC Background

- FTC is an independent law enforcement agency
- Consumer protection and competition mandate
- Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices”
- Commission brings law enforcement actions in federal or administrative court
- Commission also does policy work – public workshops, Congressional testimony, consumer education, and guidance to business
- Privacy has been a key consumer protection priority

FTC Act – Section 5 Fundamentals

- Section 5 of the Federal Trade Commission Act broadly prohibits “unfair or deceptive acts or practices in or affecting commerce.”
  - Deception → a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances
  - Unfairness → practices that cause or are likely to cause substantial injury to consumers that are not outweighed by countervailing benefits to consumers or competition and are not reasonably avoidable by consumers.
- Flexible law that can be applied to many different situations, entities, and technologies.

BUREAU of CONSUMER PROTECTION
BUSINESS CENTER

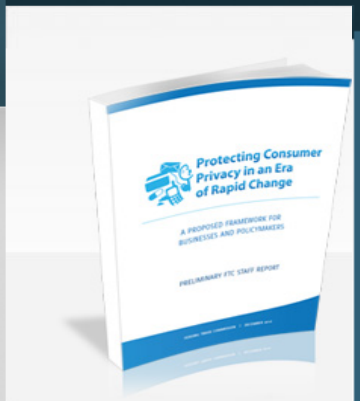
Federal Trade Commission
Protecting America's Consumers

Search this Site GO

ADVERTISING & MARKETING | CREDIT & FINANCE | PRIVACY & SECURITY | SELECTED INDUSTRIES | LEGAL RESOURCES | BUSINESS CENTER BLOG

- Multimedia
- En español

- Behavioral Advertising
- Children's Online Privacy
- Credit Reports
- Data Security
- Gramm-Leach-Bliley Act
- Health Privacy
- Red Flags Rule



er Privacy
Change
s a new

2 3 4 5 6

BUSINESS CENTER BLOG

LOANMOD TXT MSGS VIOL8 LAW, SEZ FTC

February 23, 2011

The FTC has gone to court in an effort to shut down an operation that allegedly blasted consumers with more than five million illegal spam text messages, including many pitching loan modification help, debt relief, and other services. The... READ MORE

VIEW BLOG

TOPICS

Jewelry Non-Profits Credit Reports Advertising and Marketing Red Flags Rule Online Advertising and Marketing Credit Health Claims Advertising and Marketing Basics Alcohol Franchises and Business Opportunities Real Estate and Mortgages Selected Industries Gramm-Leach-Bliley Act Clothing and Textiles Telemarketing Children's Online Privacy Tobacco Funerals Behavioral Advertising Finance Human Resources Data Security Health Privacy Privacy and Security Appliances Credit and Finance Automobiles Debt

ADVERTISING & MARKETING

The CAN-SPAM Act: A Compliance Guide for Business

Do you use email in your business? The CAN-SPAM Act establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.

TOPICS: ADVERTISING AND MARKETING, ONLINE ADVERTISING AND MARKETING, PRIVACY AND SECURITY

CREDIT & FINANCE

Complying with the Credit Practices Rule

If your company is a creditor subject to FTC jurisdiction, the Credit Practices Rules applies to you. Read this guide to find out what the Rule requires and what transactions are covered.

TOPICS: CREDIT, AUTOMOBILES, FINANCE, CREDIT AND FINANCE, SELECTED INDUSTRIES

PRIVACY & SECURITY

How to Comply with the Children's Online Privacy Protection Rule

The Children's Online Privacy Protection Act (COPPA) sets out guidelines about the online collection of personal information from children under 13. If you run a website targeting this age group – or know you're collecting information from kids – is your site COPPA compliant?

TOPICS: ADVERTISING AND MARKETING, CHILDREN'S ONLINE PRIVACY, ONLINE ADVERTISING AND

Privacy Roundtables

- Three public roundtables to explore privacy in light of new technologies, including social media
- Significant public participation
  - 200 participants reflecting range of perspectives
  - Transcripts and comments on FTC's website

Roundtable Themes

- Increased collection and use of consumer data
- Lack of understanding and informed consent
- Consumers are interested in privacy
- Benefits of data collection and use
- Decreasing relevance of PII/non-PII distinction

Privacy Report

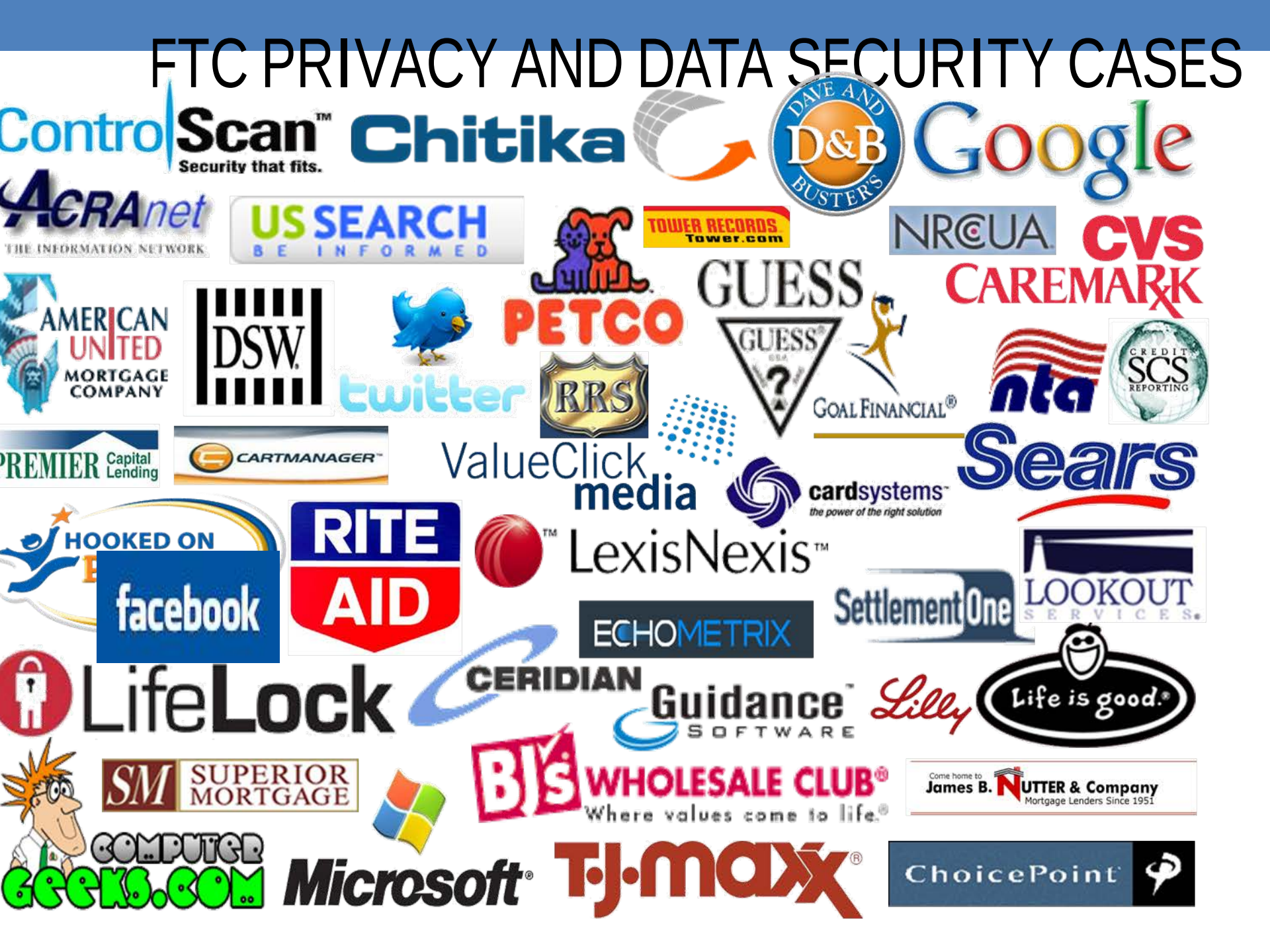
- Issued Final Report, March 2012

- Key elements:
  - Privacy by Design
  - Simplified Choice
  - Greater Transparency

Anatomy of a FTC Investigation

- Finding cases
- Pre-search
- Civil Investigative Demand or access letter
- Analyzing the facts
- Litigation or consent negotiation (or closing letter)
- Compliance and monitoring

FTC PRIVACY AND DATA SECURITY CASES



Recent Actions . . .

- Facebook
- Chitika
- RockYou
- Rite Aid

Information Security -- Four Points that Guide the FTC's Enforcement

- Information security is an ongoing process.
- A company's security procedures must be reasonable and appropriate in light of the circumstances.
- A breach does not necessarily show that a company failed to have reasonable security measures – there is no such thing as perfect security.
- A company's practices may be unreasonable and subject to FTC enforcement even without a known security breach.

Health Breach Notification Rule

- Part of the American Recovery and Reinvestment Act of 2009

- Requires covered entities that suffer a breach to:
  - Notify everyone whose information was breached;
  - In some cases, notify the media; and
  - Notify the FTC

Health Breach Notification Rule

- **Who is covered?**
  - **Vendors of personal health records (PHRs)**
    - You are a vendor of personal health records if you offer or maintain a personal health record
  - **PHR related entities**
    - You are a PHR related entity if you (1) offer products or services through a website of a PHR vendor (2) access information in a PHR or (3) send information to a PHR
  - **Third-party service providers**
    - You are a third-party service provider if you offer services to a PHR vendor or PHR related entity involving the use, maintenance, disclosure, or disposal of health information

Health Breach Notification Rule

- What triggers notification?
  - You must provide notice when there has been the **unauthorized acquisition** of **PHR-identifiable health information** that is **unsecured** and in a **personal health record**

Questions?

- Cora Tung Han, chan@ftc.gov
- www.business.ftc.gov