

DATA SECURITY, PRIVACY, AND ONLINE ENFORCEMENT AT THE U.S. FTC



Deon Woods Bell
Office of International Affairs
U.S. Federal Trade Commission
September 2015 - Trinidad and Tobago

PRESENTATION OVERVIEW

- I. FTC's Authority/Jurisdiction
- II. Data Security Principles
- III. Privacy
- IV. E-Commerce
- V. Case Studies
- VI. International Enforcement Cooperation

The views expressed are those of the speaker and not necessarily those of the FTC or its Commissioners.

I. FTC's Jurisdiction



The FTC enforces the FTC Act, which prohibits
UNFAIR and DECEPTIVE practices

- Section 5 prohibits:

- “Unfair methods of competition”

- “Unfair or deceptive acts or practices”

- Deceptive practices

- Material representation or omission that is...
- likely to mislead consumers...
- who are acting reasonably under the circumstances

- Unfair practices

- substantial injury that is...
- not reasonably avoidable and...
- not outweighed by benefits

I. FTC's Jurisdiction

- The FTC has used its authority under the FTC Act to require companies to:
 - **Maintain “reasonable procedures”** to protect sensitive consumer information
 - **Honor any promises** they make regarding the privacy or security of their information.

II. Data Security Principles

Basic Principles

- Assessment of Data Practices & Vulnerabilities, including Third Parties
- Limitation on Collection/Retention
- Physical/Technical/Administrative Protection
- Proper Disposal Policies/Practices
- Plan for Security Breaches

II. Data Security Principles

Basic Principles

The FTC has brought about 55 data security enforcement actions

- Assessment of Data Practices & Vulnerabilities, including Third Parties
- Limitation on Collection/Retention
- Physical/Technical/Administrative Protection
- Proper Disposal Policies/Practices
- Plan for Security Breaches

II. Data Security Principles

Reasonableness

- The FTC does not expect “perfect security”
- Reasonable and appropriate security is a **continuous process of assessing and addressing risks**
- There is **no one-size-fits-all** data security program

II. Data Security Principles

Reasonableness

- A company's data security measures must be reasonable and appropriate in light of:
 - the sensitivity and volume of consumer information it holds
 - the size and complexity of its business
 - the cost of available tools to improve security and reduce vulnerabilities

II. Data Security Principles

Reasonableness

- The mere fact that a breach occurred does not mean that a company has violated the laws.
- Conversely, the lack of a breach is not conclusive proof that a company's practices are adequate.

III. Privacy

- The FTC has brought enforcement actions addressing a wide range of privacy issues, including spam, social networking, behavioral advertising, pretexting, spyware, peer-to-peer file sharing, and mobile.
- These matters include over 130 spam and spyware cases and more than 40 general privacy lawsuits.

III. Privacy

Brightest Flashlight®

Android App by GoldenShores Technologies, LLC

Recent Cases:

- Goldenshore Technologies
- Aaron's, Inc.
- Snapchat
- Path
- Epic Marketplace
- Nomi Retail Tracking



III. Privacy

CHILDREN'S PRIVACY (COPPA)

- COPPA requires websites/apps directed at children to obtain parental consent before collecting personal information from children under age 13.
- Updated in July 2013 to address the rise of social networking, smartphones, and geolocation data.
- Recent Settlement: Path (social networking)
- Yelp
- TinyCo



III. Privacy

CREDIT REPORTING AND FINANCIAL PRIVACY

Enforcement of the Fair Credit Reporting Act (FCRA) and Gramm-Leach-Bliley (“GLB”) Act has resulted in liable companies paying over \$30 million in civil penalties.

Recent Cases:

- InfoTrack
- Instant Checkmate
- TimeWarner Cable
- Warning Letter issued to Data BrokersCertegy
- Filiquarian
- TeleCheck Services



III. Privacy



III. Privacy

WHY DOES THE FTC CONSIDER GEOLOCATION DATA TO BE “SENSITIVE”?

- It can reveal consumer’s movements in real time
- It can provide detailed comprehensive record of consumer’s movements over time
- It can reveal other personally identifiable info
- Unauthorized access or inappropriate use can result in harm to consumers (stalking/domestic violence, hackers using personal information to facilitate social engineering)

III. Privacy

FTC TESTIMONY ON PROPOSED LOCATION PRIVACY PROTECTION ACT OF 2014

- Supports goals of improving *transparency of geolocation* services and providing consumers with *greater control* over the collection of geolocation information.
- Supports particular aspects, such as:
 - **Definition of geolocation information** = “sufficient to identify the street name and name of the city or town” in which a device is located (consistent with COPPA).
 - The requirement that entities collecting consumer geo ***disclose*** such collection.
 - The requirement that companies get ***affirmative express consent*** from consumers before a covered entity may collect or disclose geolocation information

III. Privacy

U.S. – E.U. SAFE HARBOR

- Voluntary Framework enabling businesses to transfer personal data from the E.U. to the U.S. in a manner consistent with European adequacy standards of privacy.
 - Notice
 - Choice
 - Onward Transfer
 - Security
 - Access
 - Data Integrity
 - Enforcement

The FTC has used Section 5 to bring **26 Safe Harbor cases, including against Google and Facebook**. Also, against **TRUSTe** for misrepresentations regarding certifications.

III. Privacy

RULEMAKING

- Health Breach Notification Rule
- Telemarketing Sales Rule (TSR, robocalls, Do Not Call)
- Controlling the Assault of Non-Solicited Pornographic and Marketing (CAN-SPAM) Rule
- Fair and Accurate Credit Transactions Act of 2003 (FACTA) Rules
- Red Flags Rule

III. Privacy

REPORTS & SURVEYS

- [Internet of Things](#) (January 2015)
- [Data Brokers : A Call for Transparency](#) (May 2014)
- [Privacy Report](#) (March 2012)
- [Mobile Privacy Disclosures: Building Trust Through Transparency](#) (February 2013)
- [Paper, Plastic...or Mobile?: An FTC Workshop on Mobile Payments](#) (March 2013)
- [Mobile Apps for Kids: Current Privacy Disclosures are Disappointing](#) (February 2012)
- [Disclosures Still Not Making the Grade](#) (December 2012)

III. Privacy

WORKSHOPS

- **Spring Privacy Series** (February - May 2014)
 - [Internet of Things – Privacy and Security in a Connected World](#) (November 2013)
 - [Mobile Security: Potential Threats and Solutions Forum](#) (June 2013)
 - [Senior Identity Theft: A Problem in this Day and Age](#) (May 2014)
- **Start with Security Series** (September 2015 - ongoing)
 - [Data Security - Start-ups and Developers](#) (September 2015)
 - [Cross Device Tracking](#) (November 2015)
- **PrivacyCon** (January 2016)

III. Privacy

WORKSHOPS/CONFERENCES

- **Spring Privacy Series** (February - May 2014)
 - [Mobile Device Tracking](#) (February 19 2014)
 - [Alternative Scoring Products](#) (March 2014)
 - [Consumer Generated and Controlled Health Data](#) (May 2014)
- **Start with Security Series** (September 2015 - ongoing)
 - [Data Security - Start-ups and Developers](#) (September 2015)
 - [Cross-Device Tracking](#) (November 2015)
- **PrivacyCon** (January 2016)

III. Privacy

CONSUMER EDUCATION AND BUSINESS GUIDANCE

- Educating consumers and businesses about the ongoing threats to privacy and information security is critical to the FTC's mission.
- [OnGuardOnline.gov](https://www.onguardonline.gov)
- Start with Security Blogpost

NET CETERA
Chatting with Kids About
Being Online

OnGuardOnline.gov

IV. E-Commerce



The FTC enforces the FTC Act, which prohibits
UNFAIR and DECEPTIVE practices

- Section 5 prohibits:

- “Unfair methods of competition”

- “Unfair or deceptive acts or practices”

- Deceptive practices

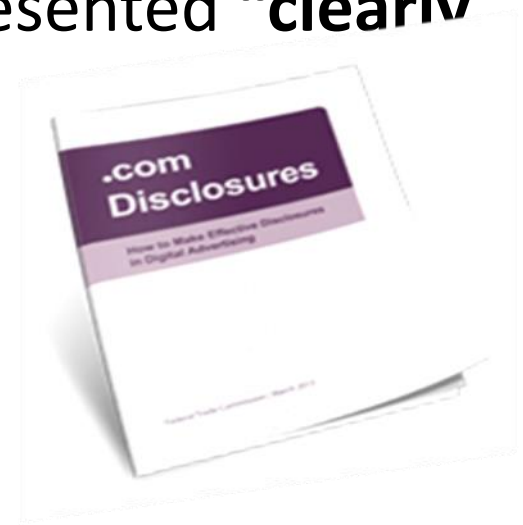
- Material representation or omission that is...
- likely to mislead consumers...
- who are acting reasonably under the circumstances

- Unfair practices

- substantial injury that is...
- not reasonably avoidable and...
- not outweighed by benefits

IV. E-Commerce

- Whether you advertise on smartphones or social media, on Twitter or through an app, the details of the deal must be up front -
 - Disclosures may be **required** to prevent an ad from being deceptive or unfair.
 - Required disclosures must be presented “**clearly and conspicuously.**”



IV. E-Commerce

.com Disclosures: Key Considerations

- When practical, advertisers should incorporate relevant limitations and qualifying information into the underlying claim, rather than having a separate disclosure qualifying the claim.
- Proximity increases the likelihood that consumers will see the disclosure and relate it to the relevant claim or product. To make conspicuous disclosures, advertisers should place disclosures as close as possible to the triggering claims.
- Disclosures that are integral to a claim should be on the same page and immediately next to the claim – especially certain cost, health, and safety disclosures. Hyperlinks should not be used to communicate such information.

IV. E-Commerce

.com Disclosures: Key Considerations (continued)

- When using a hyperlink to lead to a disclosure, advertisers should label the hyperlink appropriately to convey the importance, nature, and relevance of the information to which it leads.
- Advertisers should take account of the various devices and platforms consumers may use to view advertising and any corresponding disclosure. If an ad is viewable on a particular device or platform, any necessary disclosures should be sufficient to prevent the ad from being misleading when viewed on that device or platform. If a particular device or platform does not permit a necessary disclosure to be made effectively, that device or platform should not be used to disseminate that ad.

IV. E-Commerce

POM Wonderful – Substantiation



- The Commission found that experts in the relevant fields would require RCTs (*i.e.*, properly randomized and controlled human clinical trials) to establish a causal relationship between a food and the treatment, prevention, or reduction of risk of the serious diseases at issue in the case.

IV. E-Commerce

The FTC's Endorsement Guides What People Are Asking

FTC Endorsement Guides (April 2013)

<https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking>

- If there's a connection between an endorser and the marketer that consumers would not expect and it would affect how consumers evaluate the endorsement, the guides state that the connection should be disclosed.
- Applies to advertising in social media



IV. E-Commerce

Fake News Website Cases

Daily News - Diet Trends: A look at America's Top Diets

Exhibit A

Advertorial



CONSUMER NEWS

REPORTER

Foods that Fuel Weight Loss

"Super foods are becoming a real source in the battle to fight fat..."

Acai Berry Diet Exposed: Miracle Diet or Scam?

As part of a new series: "Diet Trends: A look at America's Top Diets" we examine consumer tips for dieting during a recession

Tuesday, January 04, 2011

» **RELATED VIDEOS**

Super foods: How to Balance your Body.

AS SEEN ON: **Consumer Reports**



Julia investigates the Acai Berry diet to find out for herself if this super diet works.

Acai berries are the latest weight loss fad. These so called Super Foods that you take as a supplement to lose weight have been getting a lot of international attention. And like you have probably already seen; they are all over the internet in blogs and success stories of people who have apparently used the pills and lost a ton of weight. But we here at News 6 are a little skeptical and aren't sure that we've seen any real proof that these pills work for weight loss. So we decided to put these products to the test. What better way to find out the truth than to conduct our own study?

To get started, I volunteered to be the guinea pig. I applied for a bottle of the [LeanSpa Acai](#).

While there are tons of Acai berry ads online, [LeanSpa Acai](#) is one of the most credible and trustworthy suppliers on the market. It included the Free trial of the product and it did not try to fool me into agreeing to additional hidden offers. Another reason why I chose [LeanSpa Acai](#) is because it is the most concentrated and purest acai products on the market. This would give me the most accurate results for my test.



Health and Diet writer, Julia Millar of the News 6 team recently put the Acai Diet to the test. She spent four weeks testing the effects of America's Newest Superfood combined with a Colon Cleanse to see for ourselves what this diet was all about. And, the results were surprising

She lost 25lbs in 4 weeks.

The benefits of the Acai berry diet beat all of our initial skepticism. We found the diet not only with weight loss, but it seemed to boost

Change your approach to living better. Why it is important to learn how to balance your diet.

The Real Dangers of having a Toxic Colon

Special CBS new report on the importance of colon health. Why it's important to remove toxins from your colon.

» **ADVERTISEMENTS**

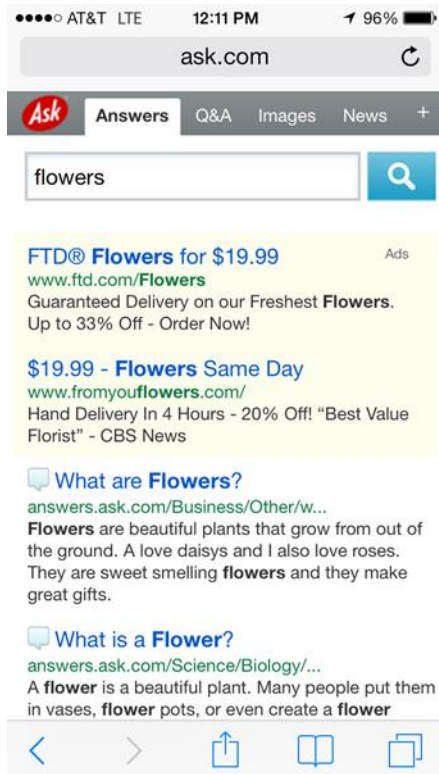
IV. E-Commerce

[December 5, 2013 Workshop on Native Advertising/Sponsored Content](#)



IV. E-Commerce

FTC Staff Guidance to Search Engines



- 2002: Original Search Engine Guidance to make clear advertisers distinguished between paid and unpaid listings
- June 2013: 24 letters sent to general search engine companies (e.g., AOL, Ask, Bing, Blekko, Duck Duck Go, Google, Yahoo) and 17 of the most heavily trafficked shopping, travel and local search engines) on distinguishing paid search results and other forms of advertising from natural search results so as to not mislead consumers.
- Discussed how visual cues, labels, or other techniques should effectively distinguish paid results from natural search.

IV. E-Commerce

Drip Pricing & Charges Undisclosed Online



<http://www.ftc.gov/os/2013/06/130625searchenginegeneralletter.pdf>

- Warning letters to 22 online hotel operators about inadequately disclosed mandatory fees hotels charge.
- The quoted total price should include any unavoidable and mandatory fees, such as resort fees, that consumers will be charged to stay at the hotel.


IV. E-Commerce

Mobile Example: Pinch & Zoom


Eye on Your Home

Login or Register | About Us | Certification

Call us now 1-800-XXX-XXXX



Keep an Eye on Your Home for Safety and Security



*Usage requires a \$9.99 monthly service fee.


Do you worry that the nanny is putting your toddler in front of the television for hours, instead of reading to her? Or do you have older children who come home to an empty house after school? An elderly parent at home alone? Or do you just want to see what the dog does while you're at work?

Get our wireless home monitoring system!

Price: \$99.99* per camera [Buy Now](#)

Set up our cameras wherever you need them, and relax. You'll be able to check on everyone and everything wherever you are, using either your computer, tablet, or smartphone equipped with our [free Eye app](#).

Our wide-angle cameras can be wall mounted or free standing. [See camera specifications.](#)



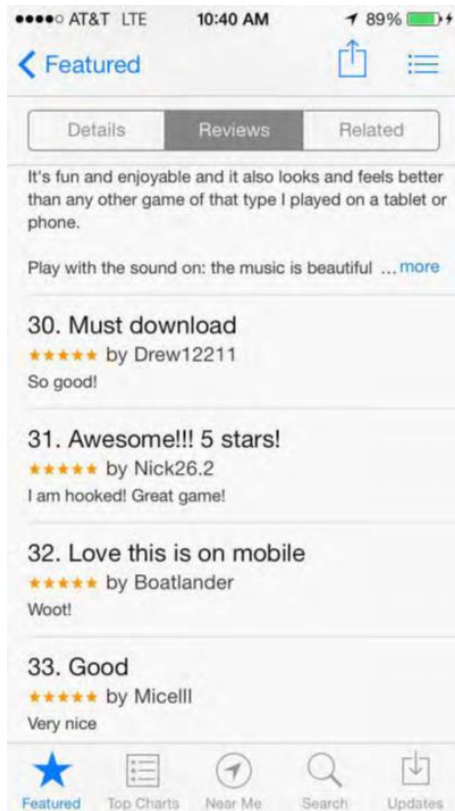
"My 80 year-old mother lives with us. I was always worried about her when I was out of the house because she had a bed fall last year. With Eye-On-Your-Home cameras in the kitchen and the family room, I can just check my smart phone when I'm out and know she's okay."

- Julie Brown
Satisfied Customer

Contact Us | Privacy Policy | Terms of Service

IV. E-Commerce

Mobile Enforcement Actions



← Reverb
Acne Apps →



IV. E-Commerce

Mobile Example: Pinch & Zoom (continued)



Mobile screen (no zooming)



Mobile screen (zoomed-in)



onguardonline.gov



and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.

- Home
- Topics
- About Us
- File a Complaint
- Resources
- Español

Learn About...



LAPTOP SECURITY

Your laptop can help you work and keep in touch, no matter where you are. It's convenient - but are you doing all you can to keep your laptop in your hands (and out of the hands of others)? Learn the steps you can take to help keep your laptop safe.

[READ MORE](#)

- Online Shopping
- POP File-Sharing
- VoIP
- Cross-Border
- Investing Online

MISSION: LAPTOP SECURITY

Test Your Knowledge, Click to Play!



Coordinating Virus & Spyware Defense

NEW TO FIGHT HIDDEN SECURITY

Get Email Alerts

Get **free alerts** from Homeland Security's U.S. Computer Emergency Readiness Team.

[READ MORE](#)

Step - Think - Click

You can minimize the chance of an Internet mishap by adopting these practices:

- 1 Protect your personal information. It's valuable.
- 2 Know who you're dealing with.
- 3 Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly.
- 4 Make sure your operating system and Web browser are set up properly and update them regularly.
- 5 Protect your passwords.
- 6 Back up important files.
- 7 Learn who to contact if something goes wrong online.

[READ MORE](#)

Word of the Day

RAM

Short-hand for "Random Access Memory," it's the hardware inside your computer that retains memory on a short-term basis and stores information while you work.

[GLOSSARY](#)



Teach Kids Online Safety

[Play & Learn](#)

<http://www.onguardonline.gov/>

ADMONGO .gov

BETA

Live the adventure.

Welcome to Admongo where advertising is all around you. Online. Outside. On television. Who makes ads? How do they work? What do they want you to do? Here, you will explore, discover, and learn. Can you make it to the top?

To get there, you'll answer:
Who is responsible for the ad?
What is the ad actually saying?
What does the ad want me to do?

[play now](#)

[Login](#)

[Watch the Trailer](#)

[Text Version](#)

Get all the learning, quickly



V. Enforcement Case Study: GMR Transcription Services



BACKGROUND

<https://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it>

- Transcription services for individuals and businesses in a variety of professions and industries
- Business conducted almost entirely online: customers upload audio files

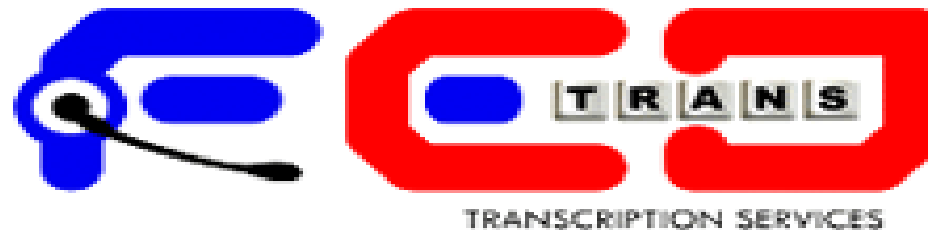


V. Enforcement Case Study: GMR Transcription Services



THIRD PARTY PROVIDERS

- Independent service providers transcribe audio files
- Medical audio file transcriptions assigned to FedTrans in India
- Files then assigned to independent typists



V. Enforcement Case Study: GMR Transcription Services



FTC COMPLAINT ALLEGATIONS

- DECEPTION:

GMR represented that it maintained reasonable practices to protect against unauthorized access, *but it did not.*

GMR represented that it took reasonable measures to oversee service providers complied with security & privacy requirements, *but it did not.*

V. Enforcement Case Study: GMR Transcription Services



FTC COMPLAINT ALLEGATIONS

- UNFAIR ACT OR PRACTICE:
 - (1) Failure to employ **reasonable and appropriate measures** to prevent unauthorized access
 - (2) Failure **caused, or was likely to cause, substantial injury**
 - (3) Injury **not outweighed by benefits** to consumers
 - (4) Injury **not reasonably avoidable by consumers**

V. Enforcement Case Study: GMR Transcription Services



SECURITY FAILURES

- Failure to **request or review** relevant information about security practices:
 - A written information security program
 - Audits/assessments of its computer network.
- Inadequate **verification** of provider's security measures
- Failure to **monitor and periodically assess** effectiveness of provider's practices

V. Enforcement Case Study: GMR Transcription Services



SECURITY FAILURES

- Failure to ensure **by contract** that provider adopt and implement appropriate security measures, such as:
 - Secure storage/transmission (*e.g.*, through encryption)
 - Authentication of contractors (*e.g.*, through unique user credentials)

V. Enforcement Case Study: GMR Transcription Services



CONSIDERATIONS

- No breach, but substantial potential for injury
- Availability of low-cost security measures
- No way for consumers to discover security vulnerabilities

V. Enforcement Case Study: GMR Transcription Services



PROPOSED CONSENT ORDER

- Comprehensive data security program:
 - Designate accountable coordinator
 - Identify internal/external security risks
 - Design/Implement safeguards
 - Select/retain capable providers
 - Contractual arrangement w/ providers
 - Evaluate/Test/Monitor/Adjust
 - Independent Audits for 20 years

V. Enforcement Case Study: Wyndham

FTC v. WYNDHAM WORLDWIDE CORPORATION



Background

- Hospitality company that franchises and manages hotels through three subsidiaries
 - Wyndham has licensed its brand name to approximately 90 independently owned hotels
- Each hotel has a property management system that processes personal consumer information

V. Enforcement Case Study: Wyndham

SECURITY FAILURES

1. Allowed Wyndham-branded hotels to store payment card information in clear readable text.
2. Used easily guessable passwords to access property management systems
3. Failed to use readily available security measures such as firewalls to limit access between the hotels' property management systems and corporate network
4. Failed to remedy known security vulnerabilities

V. Enforcement Case Study: Wyndham

SECURITY FAILURES

5. Failed to adequately inventory computers in order to properly manage the devices on its network
6. Failed to employ reasonable measures to detect and prevent unauthorized access to network or to conduct security investigations
7. Failed to follow proper incident response procedures, including failing to monitor computer network for malware used in a previous intrusion
8. Failed to adequately restrict third-party vendors' access to network

V. Enforcement Case Study: Wyndham

THREE BREACHES 2008-2009

1. April 2008 – Hackers used the brute-force method to steal unencrypted information from over 500,000 accounts
2. March 2009 – Hackers gained access to nearly 40 property management servers on the network.
3. Late 2009 – Failure to properly implement firewalls allowed hackers to break in a third time and steal about 69,000 card numbers



V. Enforcement Case Study: Wyndham

FTC COMPLAINT ALLEGATIONS

DECEPTION

- Wyndham privacy statement led consumers to believe their personal information was safeguarded from unauthorized access

“We safeguard our Customers’ personally identifiable information by using **industry standard practices**. Although ‘guaranteed security’ does not exist either on or off the Internet, **we make commercially reasonable efforts** to make our collection of such Information consistent with all applicable laws and regulations.”

-Wyndham privacy statement

V. Enforcement Case Study: Wyndham

FTC Files Complaint Against Wyndham Hotels For Failure to Protect Consumers' Personal Information

Credit Card Data of Hundreds of Thousands of Consumers Compromised, Millions of Dollars Lost to Fraud

FOR RELEASE

June 26, 2012

FTC COMPLAINT ALLEGATIONS

Unfairness

- Wyndham's actions caused substantial injury to 619,000 consumers whose information was stolen
 - Injury not reasonably avoidable by consumers who believed their personal information was safely stored

V. Enforcement Case Study: Wyndham

NATIONAL LAW REVIEW

In Commission Win, Appeals Court Agrees that FTC Can Regulate Business Data Security Practices Under Unfairness Authority

3rd Circuit Court of Appeals Decision (August 2015)

- Affirmed district court's denial of Wyndham's motion to dismiss
 - "Today's Third Circuit Court of Appeals decision reaffirms the FTC's authority to hold companies accountable for failing to safeguard consumer data. It is not only appropriate, but critical, that the FTC has the ability to take action on behalf of consumers when companies fail to take reasonable steps to secure sensitive consumer information."
–Edith Ramirez

VI. International Cooperation



- **ENFORCEMENT COOPERATION**
 - Global Privacy Enforcement Network (GPEN)
 - APEC Cross-border Privacy Enforcement Arrangement (CPEA)
 - International Consumer Protection and Enforcement Network (ICPEN)
 - London Action Plan (LAP)

VI. International Cooperation



GLOBAL PRIVACY POLICY COOPERATION

- FTC advocates for policies that ensure consumer data transferred outside of the U.S. and across national borders is adequately protected.
 - Organization for Economic Cooperation and Development issued revised Guidelines governing the Protection of Privacy and Trans-border Flows of Personal Data (July 2013)

Questions/Comments?



- More information available at:
www.ftc.gov

Contact:

Deon Woods Bell

dwoodsbell@ftc.gov

202-326-3307

