Federal Trade Commission

Privacy and Data Security at the Federal Trade Commission: Recent Developments

Remarks of Joshua D. Wright*
Commissioner, Federal Trade Commission

at

Forum for EU-US Legal-Economic Affairs

The Mentor Group
Brussels, Belgium
April 8, 2014

I. Introduction

Good afternoon. I would like to thank Thomas Kosmo and the Mentor Group for the generous invitation to join this distinguished group and to participate in the Brussels Forum for EU-US Legal-Economic Affairs. I am pleased to have the opportunity to discuss the Federal Trade Commission's (FTC) recent enforcement

* The views stated here are my own and do not necessarily reflect the views of the Commission or other Commissioners. I am grateful to my advisor, Beth Delaney, for her invaluable assistance in preparing this speech.

efforts addressing the privacy and data security of consumer information and how these enforcement actions might help inform privacy legislation in the European Union.

As many of you are aware, in the United States, there isn't just one law or statute that broadly regulates the privacy and data security of consumer information. Instead, our privacy and data security framework consists of an array of federal laws which identify and regulate specific areas of concern and are enforced by a range of federal agencies that often operate in tandem with state legislative regimes. These federal laws, and the rules promulgated pursuant to them, are designed to protect consumers from harms associated with certain types of consumer information that are procured through transactions with specified entities. For example, sensitive health information is covered by the Health Insurance Portability and Accountability Act (HIPAA), financial information is regulated by the Gramm-Leach-Bliley Act (GLB Act), information used to make credit, insurance and employment decisions falls under the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA), and personal information collected online from children under the age of 13 is regulated by the Children's Online Privacy Protection Act (COPPA).

Each of these laws enumerates specific requirements and protections for the handling of the particular type of personal information at issue -- including provisions regarding the collection, disclosure, security, maintenance, and deletion of such information -- by entities such as financial institutions, healthcare providers, credit

reporting agencies, and websites. Some of these laws also require consumer access to the information and allow consumers to correct that information if it is inaccurate. The Commission, alone or in coordination with other agencies, routinely brings privacy and data security cases using these laws.[1]

Certegy Check Services, a case brought by the FTC last August against one of the United States' largest check authorization service companies, illustrates some of these concepts.[2] Certegy is a consumer reporting agency (CRA) that compiles consumers' personal information and uses it to help retail merchants determine whether to accept consumers' checks. Under the FCRA, consumers whose checks are denied based upon information Certegy provides the merchant have the right to dispute that information and to have Certegy correct any inaccuracies.

The FTC alleged in its complaint that Certegy did not follow proper dispute procedures and also failed to follow reasonable procedures to assure the accuracy of the information it provided to its merchant clients, as required by the FCRA. *Certegy* was the first Commission action alleging violations of the Furnisher Rule, which was

---

[1] *See, e.g.*, Rite Aid Corp., F.T.C. File No. 0723121 (Nov. 12, 2010) (consent order) (in conjunction with the Department of Health and Human Services; alleging failure to establish policies and procedures for the secure disposal of consumers' sensitive health information) (HIPAA); SettlementOne Credit Corp., F.T.C. File No. 0823208 (Feb. 9, 2011) (proposed consent agreement) (alleging that credit report reseller failed to implement reasonable safeguards to control risks to sensitive consumer information) (GLB Act); United States v. Playdom, Inc., Case No. SACV 11-0724-AG(ANx) (C.D. Cal. May 24, 2011) (consent order) (alleging failure to provide notice and obtain consent from parents before collecting, using, and disclosing children's personal information) (COPPA).

[2] United States of America et al v. Certegy Check Services, Inc., No. 1:13-cv-01247 (D.D.C. 2013).

promulgated under the FCRA and went into effect on July 1, 2010. That rule requires that credit reporting agencies such as Certegy must establish and implement reasonable written policies and procedures regarding the accuracy and integrity of information furnished to other CRAs. Certegy Check Services agreed to pay $3.5 million to settle these allegations.

In addition to -- and in contrast with -- these very specific and circumscribed laws, the Federal Trade Commission also exercises its authority to combat the mishandling of consumers' sensitive personal information through the "unfair or deceptive acts or practices" prong of Section 5 of the FTC Act. An act or practice is unfair if "it 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 competition."[3] An act or practice is deemed deceptive "if there is a misrepresentation, omission, or other practice, that misleads the consumer acting reasonably in the circumstances, to the consumer's detriment."[4]

II. The Evolution of the Commission's Deception Authority in the Privacy and Data Security Context

The genesis of the Commission's online privacy program dates back to 1998, just over 15 years ago, when the agency brought a deception case against one of the most

[3] 15 U.S.C. § 45(n).

[4] Fed. Trade Comm'n, Policy Statement on Deception, *reprinted at* 103 F.T.C. 174-5 (1984) [hereinafter Deception Statement].

popular websites on the Internet at that time -- GeoCities -- a website that provided services such as personal home pages and email services to its members. In order to become a member of GeoCities, individuals had to complete an online application form that requested certain personally identifiable information, some information was mandatory while other information was "optional." Using this registration process, GeoCities created a database that included email and postal addresses, member interest areas, and demographics including income, education, gender, marital status, and occupation. However, as set forth in the FTC's complaint, GeoCities misrepresented to its members not only how it would use the information, but also that the "optional" information would not be released to anyone without the member's permission.

Many of the Commission's subsequent privacy cases in this early era also were based upon similar fact patterns and alleged deception – despite making certain representations in their privacy policies that consumers' personal information would not be shared or disclosed, defendants failed to honor these representations.[5] Around the same timeframe, the Commission also began examining representations that

[5] *See, e.g.*, FTC v. Toysmart.com, LLC, No. 00-11341-RGS, 2000 WL 34016434 (D. Mass. July 21, 2000) (consent order) (challenging website's attempts to sell children's personal information, despite a promise in its privacy policy that such information would never be disclosed); and In re Liberty Fin. Cos., 128 F.T.C. 240 (1999) (consent order) (alleging that site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously).

companies were making about the security of the consumer information that they were handling.[6]

Perhaps one of the most notable cases during this early timeframe on the data security front was *Eli Lilly*. Lilly is a pharmaceutical company that provided consumers with an email reminder service whereby consumers could design and receive personal email messages to remind them to take or refill their prescription medications, in this case, the antidepressant Prozac. However, in the process of announcing the termination of this service, Lilly sent out one final email that included all recipients' email addresses in the "To" line of the message, thereby unintentionally disclosing to each individual subscriber the email addresses of all 669 subscribers (and most likely Prozac users).

Lilly's privacy policies had informed consumers that Lilly recognized the importance of keeping sensitive information private and that it took measures to do so. In light of the email address incident, the FTC complaint therefore alleged that Lilly's claim of privacy and confidentiality was deceptive because Lilly failed to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information.[7]

---

[6] FTC v. Sandra Rennert, No. CV-S-00-0861-JBR (D. Nev. July 6, 2000) (consent order) (alleging that defendants misrepresented the security and encryption used to protect consumers' information and used the information in a manner contrary to their stated purpose).

[7] In the Matter of Eli Lilly and Co., F.T.C. File No. 0123214 (May 10, 2002) (complaint), *available at* http://www.ftc.gov/os/2002/05/elililllycmp.htm.

This brief background on the agency's use of deception in bringing privacy and data security enforcement cases is useful in providing a historical context to highlight the challenges that the FTC now faces in protecting consumers as technology rapidly evolves and consumers interact with an ever-increasing variety of products and interfaces. As I will discuss further, while our recent enforcement efforts still focus largely upon deceptive statements in the privacy and data security area, the stakes are much higher. Companies have access to a greater volume of personal information, and because more and more businesses rely upon electronic communications and the Internet, these datasets may contain more sensitive data than ever before. In addition, the consumers in the modern economy have access to more products, social media sites, devices and apps, and greater opportunities for the collection and sharing of personal information. Despite this constantly changing terrain, the Commission continues to effectively protect consumers by using its Section 5 deception authority to challenge misrepresentations made by companies about the privacy or data security they afford to consumers' data, no matter what the context.

III. Recent Enforcement Cases Utilizing the Commission's Deception Authority

Late last month, the FTC announced that two companies -- Fandango and Credit Karma -- agreed to settle charges that they misrepresented the security of their mobile apps when they failed to secure the transmission of millions of consumers' sensitive

personal information from their mobile apps[8]. The Fandango Movies app for iOS allows consumers to purchase movie tickets and view show times, trailers, and reviews while the Credit Karma Mobile app for iOS and Android allows consumers to monitor and evaluate their credit and financial status.

Both of these cases alleged the same misstep – in designing their mobile apps, both Fandango and Credit Karma disabled a critical default process, known as Secure Sockets Layer (SSL) certificate validation. To help secure sensitive transactions, mobile operating systems, including iOS and Android, provide app developers with tools to implement the industry standard SSL. If properly implemented, SSL secures an app's communications and ensures that an attacker cannot intercept the sensitive personal information a consumer submits through an app. Instead, the companies' disabling of SSL left their apps vulnerable to "man-in-the-middle" attacks, which allow a third party to intercept any of the information the apps sent or received. This type of attack is especially dangerous on unsecured public Wi-Fi networks at coffee shops, airports and shopping centers, where these apps were intended to be used.

By overriding the default validation process, Fandango undermined the security of ticket purchases made through its iOS app, exposing consumers' credit card details, including card number, security code, zip code, and expiration date, as well as

[8] In the Matter of Fandango, LLC, F.T.C. File No. 1323089 (Mar. 28, 2014); In the Matter of Credit Karma, F.T.C. File No. 1323091 (Mar. 28, 2014).

consumers' email addresses and passwords. Similarly, Credit Karma's apps for iOS and Android exposed consumers' Social Security Numbers, names, dates of birth, home addresses, phone numbers, email addresses and passwords, credit scores, and other credit report details such as account names and balances.

As alleged in the complaints, the Fandango app assured consumers during checkout that their credit card information was stored and transmitted securely. Likewise, Credit Karma assured consumers that the company followed industry-leading security precautions, including the use of SSL to secure their information. Despite the fact that this vulnerability could have easily been tested for and prevented, both companies failed to perform the basic and widely available security checks that would have caught the issue.[9]

In settling these allegations, both companies have agreed to establish comprehensive security programs designed to address security risks during the development of their applications and to undergo independent security assessments every other year for the next 20 years. The settlements also prohibit Fandango and Credit Karma from misrepresenting the level of privacy or security of their products and services. These settlements have been put on the public record for a 30-day

[9] Even after a user warned Credit Karma about the vulnerability in its iOS app, the company failed to test its Android app before launch. As a result, one month after receiving a warning about the issue, the company released its Android app with the very same vulnerability. In addition, Fandango failed to have an adequate process for receiving vulnerability reports from security researchers and other third parties, and as a result, missed opportunities to fix the vulnerability.

comment period, after which the Commission will consider the comments and decide whether to finalize the settlements.[10]

In February 2013, the operator of the Path social networking app agreed to settle charges that it deceived users by collecting personal information from their mobile device address books without their knowledge and consent.[11] Path allows users to keep journals about "moments" in their life and to share that journal with a network of up to 150 friends. Through the Path app, users can upload, store, and share photos, written "thoughts," the user's location, and the names of songs to which the user is listening.

The FTC charged that the user interface in Path's iOS app was misleading and provided consumers no meaningful choice regarding the collection of their personal information. In version 2.0 of its app for iOS, Path offered an "Add Friends" feature to help users add new connections to their networks. The feature provided users with three options: "Find friends from your contacts;" "Find friends from Facebook;" or "Invite friends to join Path by email or SMS." Despite the implied representation that Path would only collect this information if you chose one of these options, Path automatically collected and stored personal information from the user's mobile device address book even if the user had not selected the "Find friends from your contacts" option. For each contact in the user's mobile device address book, Path automatically

[10] Press Release, Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers By Failing to Securely Transmit Sensitive Personal Information (Mar. 28, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers.
[11] United States of America, Plaintiff, v. Path, Inc., F.T.C. File No. 1223158 (Feb. 1, 2013).

collected and stored any available first and last names, addresses, phone numbers, email addresses, Facebook and Twitter usernames, and dates of birth.

The FTC also alleged that Path's privacy policy deceived consumers by claiming that it automatically collected only certain user information such as IP address, operating system, browser type, address of referring site, and site activity information. In fact, version 2.0 of the Path app for iOS automatically collected and stored personal information from the user's mobile device address book when the user first launched version 2.0 of the app and each time the user signed back into the account.

In addition, because Path had collected birthdates and knew these users were children, it was also charged with violating COPPA by collecting personal information from approximately 3,000 children under the age of 13 without first getting parental consent.

Similar to the Fandango and Credit Karma settlements, Path's settlement agreement with the FTC requires Path to establish a comprehensive privacy program and to obtain independent privacy assessments every other year for the next 20 years. The company also paid $800,000 in civil penalties to settle charges that it violated COPPA by illegally collecting personal information from children without their parents' consent.

In another recent case brought in January 2013, the FTC charged the operator of a leading cord blood bank, Cbr Systems, Inc., with failing to protect the security of its

customers' personal information, despite its representations to the contrary. In its privacy policy, Cbr had stated that "[w]henever CBR handles personal information, regardless of where this occurs, CBR takes steps to ensure that your information is treated securely . . . Once we receive your transmission, we make our best effort to ensure its security on our systems."[12]

However, the FTC charged that Cbr failed to provide reasonable and appropriate security for consumers' personal information and that these failures contributed to a December 2010 security breach during which unencrypted backup tapes containing consumers' personal information, a Cbr laptop, a Cbr external hard drive, and a Cbr USB drive were stolen from a Cbr employee's personal vehicle in San Francisco, California. The unencrypted backup tapes included, in some cases, the names, gender, Social Security Numbers, dates of birth, drivers' license numbers, credit and debit card numbers, card expiration dates, checking account numbers, addresses, email addresses, and telephone numbers of nearly 300,000 Cbr customers.

In its complaint, the Commission spelled out the company's shortcomings in failing to secure personal information as promised. In particular, the complaint alleged that Cbr had failed to implement reasonable policies and procedures to protect the security of the personal information it collected from consumers. Second, the company

[12] Complaint at 2, In the Matter of CBR Systems, Inc., F.T.C. Docket No. C4400 (Jan. 28, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/01/130128cbrcmpt.pdf.

had created unnecessary risks to personal information by, among other things, transporting portable media containing personal information in a manner that made it vulnerable to theft; failing to adequately supervise a service provider, resulting in the retention of a legacy database that contained consumers' personal information; failing to take reasonable steps to render backup tapes or other portable media containing personal information unusable, unreadable, or indecipherable in the event of unauthorized access; not adequately restricting access to its databases based on an employee's need for information; and failing to destroy consumers' personal information for which the company no longer had a business need. Finally, the complaint pointed out that Cbr had failed to employ sufficient measures to prevent, detect, and investigate unauthorized access to computer networks, such as by adequately monitoring web traffic, confirming distribution of anti-virus software, employing an automated intrusion detection system, or systematically reviewing system logs for security threats.[13]

[13] The settlement requires Cbr to establish and maintain a comprehensive information security program and submit to security audits by independent auditors every other year for 20 years. The settlement also bars Cbr from misrepresenting its privacy and security practices. *See also* In the Matter of ScanScout, Inc., F.T.C. File No. 1023185 (Nov. 18, 2011). In November 2011, online advertiser ScanScout agreed to settle charges that it deceptively claimed that consumers could opt out of receiving targeted ads by changing their computer's web browser settings to block cookies. In fact, ScanScout used Flash cookies, which browser settings could not block. The proposed settlement bars misrepresentations about the company's data-collection practices and consumers' ability to control collection of their data. It also requires that ScanScout take steps to improve disclosure of their data collection practices and to provide a user-friendly mechanism that allows consumers to opt out of being tracked.

While this detailed list of failures might seem to be somewhat excessive, the Commission believes that such transparency is useful not only in explaining our basis for bringing an enforcement action, but also because it serves to inform other companies about their data security obligations and to alert them as to how to bring their security systems into conformance with industry standards.

IV. The Commission's Use of its Unfairness Authority in the Online Environment

All of the cases described thus far are grounded in the FTC's deception authority -- companies have expressly or impliedly made representations about the privacy or data security that they provide for consumers' data, but in reality, their actions fell short of these promises. However, entities that handle consumer data aren't necessarily required to make representations about their practices. For example, while certain companies might be regulated by the specific statutes I discussed earlier, and therefore may be required to have a privacy policy or to treat consumer information in a particular way, other entities are not specifically regulated in this way.

The unfairness prong of the FTC's Section 5 authority allows the agency to pursue enforcement actions where there may not be a triggering representation, but a 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 competition."[14] In implementing its unfairness authority, the Commission recognizes that in deeming an act or practice as "unfair" it must undertake a cost-benefit analysis[15] – I believe that the proper approach is for the Commission to consider the security deficiencies at issue, the resultant harm to consumers, if any, and whether there were low-cost steps that would significantly reduce the risk.[16]

The Commission began exploring the use of its unfairness authority in the online context beginning around the same time that it was developing its privacy and data security cases under a deception theory. One of the first cases to allege unfairness in this new environment was brought under the stewardship of former Chairman Tim Muris and former Consumer Protection Bureau Director Howard Beales in October 2001. In the so-called *Cupcake Party* case, the Commission alleged that John Zuccarini, a cyberscammer, used more than 5,500 copycat or misspelled Web addresses to divert Internet users from their intended Internet destinations to one of his sites, and then hold them captive while he pelted their screens with a barrage of ads. It was extremely difficult for website visitors to exit from this programming, and often computers would crash and consumers could lose unsaved work product, or otherwise be deprived of the use of their computers. The Commission's complaint alleged two unfairness counts –

---

[14] 15 U.S.C. § 45(n).
[15] FTC Policy Statement on Unfairness, *appended to* Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984).
[16] *See* J. Howard Beales, III & Timothy J. Muris, Choice or Consequences: Protecting Privacy in Commercial Information, 75 U. CHI. L. REV. 132 (2008).

one for Zuccarini's practice of diverting consumers to his websites, and a second count for his practice of obstructing consumers from then leaving those websites.[17]

Another early unfairness case involving consumer information, *Gateway Learning*, involved a deliberate, unilateral breach of representations made in a company's privacy policy. The Commission alleged that the company, the maker of the popular "Hooked on Phonics" system, retroactively changed its privacy policy, without notifying consumers, to allow the company to rent customers' personal information to marketers.[18] These material changes were inconsistent with Gateway's original representations to consumers at the time the personal information was collected, and the company retroactively applied such changes to this previously-collected personal information. The FTC alleged that Gateway's retroactive application of its revised privacy policy ran afoul of the Commission's longstanding doctrine that a unilateral contract change that causes substantial injury to consumers that is not outweighed by countervailing benefits is an unfair practice under Section 5.[19]

V. Recent Use of The Commission's Unfairness Authority

The Commission has continued its trend of carefully applying its unfairness authority, while at the same time exploring new opportunities for its use. Often the

---

[17] Federal Trade Commission v. John Zuccarini, dba Cupcake Party, Civ. Action No. 201-CV-04854-BMS (E.D. Pa. 2007).

[18] In the Matter of Gateway Learning Corp., F.T.C. File No. 0423047 (consent agreement), *available at* http://www.ftc.gov/opa/2004/07/gateway.htm.

[19] Orkin Exterminating Co., 117 F.T.C. 747 (1994).

factual scenarios underlying these cases will justify allegations of both unfairness and deception.[20] The *HTC America* case brought by the Commission in February 2013 is a good example.[21]

The Commission charged that mobile device manufacturer HTC failed to employ reasonable and appropriate security practices in the design and customization of the software it developed for its smartphones and tablet computers, introducing security flaws that placed sensitive information about millions of consumers at risk. Among other things, the complaint alleged that HTC failed to provide its engineering staff with adequate security training, failed to review or test the software on its mobile devices for potential security vulnerabilities, failed to follow well-known and commonly accepted secure coding practices, and failed to establish a process for receiving and addressing vulnerability reports from third parties.

While these failures sound remarkably similar to the charges plead against Fandango and Credit Karma, in the *HTC America* case, the Commission used its Section 5 unfairness authority, in addition to its deception authority, to pursue an enforcement action against HTC for its security shortcomings. Although HTC did make some

---

[20] In the Matter of CardSystems Solutions, Inc., F.T.C. File No. 0523148 (Sept. 8, 2006) (decision and order); In the Matter of DSW, Inc., F.T.C. File No. 0123196 (Dec. 15, 2005) (stipulated final order); In the Matter of BJ's Wholesale Club, Inc., F.T.C. File No. 0423160 (Sept. 20, 2005) (decision and order); In the Matter of Guidance Software, Inc., F.T.C. File No. 0623057 (Apr. 3, 2007) (decision and order); In the Matter of LifeIsGood Retail, Inc., F.T.C. File No. 0723046 (Apr. 18, 2008) (decision and order); In the Matter of Reed Elsevier, F.T.C. File No. 0810133 (June 5, 2009) (decision and order); and In the Matter of TJX Companies, F.T.C. File No. 0723055 (Aug. 1, 2008) (decision and order).

[21] In the Matter of HTC America, F.T.C. File No. 1223049 (Feb. 22, 2013).

representations about security in its user manuals for its Android-based mobile devices, these representations did not cover all of the conduct, or all of the devices at issue.

By pleading both unfairness and deception, the Commission's complaint was able to cover all the security flaws, whether the mobile device used an Android or Windows operating system. Accordingly, the settlement agreement required HTC America to develop and release software patches to fix vulnerabilities found in millions of HTC devices and to establish a comprehensive security program designed to address security risks during the development of its mobile devices and to undergo independent security assessments every other year for the next 20 years.

The Commission also alleged unfairness and deception in its recent enforcement action against TRENDnet, a company that markets video cameras designed to allow consumers to monitor their homes remotely for purposes ranging from home security to baby monitoring. Although TRENDnet claimed that the cameras were "secure," they had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet address. This resulted in hackers posting 700 consumers' live feeds on the Internet. As with its other data security cases, the Commission listed the company's inadequacies in detail in the complaint: transmitting and storing log-in credentials in clear, readable text; failing to implement a procedure to monitor third-party vulnerability reports; and failing to failed to employ

reasonable and appropriate security in the design and testing of the software that it provided consumers for its cameras.

Under the terms of its settlement with the FTC, TRENDnet must maintain a comprehensive security program, obtain outside audits, notify consumers about the security issues and the availability of software updates to correct them, and provide affected customers with free technical support for the next two years.

The DesignerWare cases brought by the Commission over the last two years are also good illustrations of our cutting-edge enforcement efforts to target abuses of consumer privacy and data security.[22] DesignerWare is developed and then licensed its proprietary software to rent-to-own stores, including franchisees of Aaron's, ColorTyme, and Premier Rental Purchase, to help them track and recover rented computers. As alleged in our complaint, DesignerWare's software contained a "kill switch" that the rent-to-own stores could use to disable a computer if it was stolen, or if the renter failed to make timely payments. DesignerWare also had an add-on program known as "Detective Mode" that purportedly helped rent-to-own stores locate rented computers and collect late payments. DesignerWare's software also collected data that allowed the rent-to-own operators to secretly track the location of rented computers,

[22] Press Release, FTC Approves Final Order Settling Charges Against Software and Rent-to-Own Companies Accused of Computer Spying (Apr. 15, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/04/ftc-approves-final-order-settling-charges-against-software-and; Press Release, FTC Approves Final Order Settling Charges that Aaron's Inc. Allowed Franchisees to Spy on Consumers via Rental Computers (Mar. 11, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/03/ftc-approves-final-order-settling-charges-aarons-inc-allowed.

and thus the location of those using the computers. When Detective Mode was activated, the software could log key strokes, capture screen shots and take photographs using a computer's webcam.[23] It also presented a fake software program registration screen that tricked consumers into providing their personal contact information.

V. Compliance with the U.S.-EU Safe Harbor

One final area I would like to conclude with is the agency's efforts in bringing deception cases against companies that are falsely claiming they are abiding by the international privacy framework known as the U.S.-EU Safe Harbor. As you are aware, this framework enables U.S. companies to transfer consumer data from the European Union to the United States in compliance with EU law. In January, the Commission announced settlements with 12 companies representing represent a cross-section of industries, including retail, professional sports, laboratory science, data broker, debt collection, and information security.[24] These companies handle a variety of consumer information, including in some instances sensitive data about health and employment.

---

[23] Data gathered by DesignerWare and provided to rent-to-own stores using Detective Mode revealed private and confidential details about computer users, such as user names and passwords for email accounts, social media websites, and financial institutions; Social Security numbers; medical records; private emails to doctors; bank and credit card statements; and webcam pictures of children, partially undressed individuals, and intimate activities at home.

[24] Press Release, FTC Settles with Twelve Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework (Jan. 21, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply.

As set forth in the FTC's complaints, these companies deceptively claimed they held current certifications under the U.S.-EU Safe Harbor framework and, in three of the complaints, also deceptively claimed certifications under the U.S.-Swiss Safe Harbor framework. FTC Chairwoman Edith Ramirez had made clear that enforcement of the U.S.-EU Safe Harbor Framework is a Commission priority. These cases help ensure the integrity of the Safe Harbor Framework and put companies on notice that they cannot falsely claim participation in the program.

Thank you for your time.