



# Federal Trade Commission

---

## Consumer Protection Challenges and Priorities for 2014

Jessica Rich<sup>1</sup>

Director, Bureau of Consumer Protection, FTC

Consumer Federation of America

2014 Consumer Assembly

March 21, 2014

- Good morning. I am delighted to be here with my state and local colleagues. I would like to thank the CFA for having me here today to discuss the FTC's consumer protection challenges and priorities for 2014.
- The FTC protects consumers by stopping unfair, deceptive, or fraudulent practices in the marketplace. We conduct investigations, sue companies and people that violate the law, develop rules to ensure a vibrant marketplace, and educate consumers and businesses about their rights and responsibilities.
- The Commission is first and foremost a law enforcement agency. Our "bread and butter" mission falls primarily into three categories – fighting fraud, stopping deceptive advertising, and protecting consumer privacy. Within these categories, we are focusing right now on five key themes that reflect the consumer protection needs in the marketplace today: (1) mobile and connected devices; (2) "Big Data"; (3) vulnerable and targeted groups; (4) gatekeepers and facilitators; and (5) pushing for new privacy and data security laws.
- Mobile and Connected devices – The first area of focus is mobile technologies and

---

<sup>1</sup> The views expressed here are my own and do not necessarily represent the views of the Federal Trade Commission or any Commissioner. Special thanks to Molly Crawford for assisting in the preparation of these remarks.

connected devices. Over the last few years, mobile technology has become one of the main priorities for the Commission. For example:

- Mobile Unit: We created an entire Mobile Technology Unit to coordinate our enforcement, policy, and outreach focus across the entire Bureau of Consumer Protection.
- Mobile Reports & Workshops: On the policy front, the FTC has already issued several reports, including two reports showing the lack of mobile privacy disclosures in kids' apps; a report making recommendations on mobile privacy disclosures; and a mobile payments report. We also hosted a workshop on mobile security last year.
- Goldenshores: We also have brought cases challenging law violations occurring in the mobile ecosystem. For example, the FTC announced a settlement with Goldenshore Technologies, the maker of Brightest Flashlight, a popular app – installed more than 50 million times – that allows consumers to use their mobile devices as flashlights. According to the complaint, Goldenshore promised that it would collect information from users' mobile devices for certain internal housekeeping purposes, but failed to disclose that the app transmitted the device's precise location and device ID to third parties, including mobile advertising networks.
- Mobile Cramming: The Commission has also done a significant amount of work targeting mobile cramming. Last year, the Commission hosted a roundtable on mobile cramming, bringing stakeholders together to explore how mobile cramming occurs and how to protect consumers from this practice. And, following the roundtable, the Commission brought several cases challenging the placement of third-party charges on mobile bills without consumers' consent (*e.g., Wise Media, Jesta, Bullroarer*).
- Big Data – The term “Big Data” describes the vast capabilities of companies to gather data from numerous sources and combine it in ways to make inferences about people. Big Data can drive valuable innovation – for example, it can be used to track traffic patterns in order to ease congested commutes home, or even determine what medical treatments are most effective across a large population. However, the pooling of vast stores of data raises obvious risks: virtually unlimited data collection without consumer knowledge or consent; data breaches involving this treasure trove of information; and the concern that companies will make inferences about consumers that simply aren't true. Some of the recent efforts involving Big Data include:

- Internet of Things Workshop: In December, the FTC held a workshop on the “Internet of Things” – the phenomenon where consumers can connect remotely to their refrigerators, bank accounts, thermostats, cars, and many other products and devices. The workshop brought together stakeholders to explore the security and privacy issues related to increased connectivity for consumers, including areas such as smart homes, connected health and fitness devices, and connected cars. Following the workshop and a public comment period, we are developing a report to summarize the findings and, where appropriate, set forth best practices for managing privacy and security with new interconnected devices.
- Spring Privacy Series: We are in the middle of a three-part “Spring Seminar Series” to discuss several trends in Big Data and their impact on consumer privacy. The series is focusing on mobile device tracking in retail stores; the use of predictive scoring to help companies predict consumer behavior and shape how they market to particular consumers; and health apps and devices that consumers increasingly use to manage and analyze their health data.
- TRENDnet: The FTC recently announced its first “Internet of Things” case involving a video camera designed to allow consumers to monitor their homes remotely. The complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring, and claimed in numerous product descriptions that they were “secure.” In fact, the cameras 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.
- Data Broker Report: We plan release of a report on data brokers in the coming months. Data brokers collect, maintain, and sell a wealth of information about consumers, but they often do not interact directly with consumers. Rather, they get data from public records or purchase it from other companies. As a result, consumers are often unaware of the existence of data brokers, let alone the purposes for which they collect and use consumers’ data. To better understand the industry, the Commission sent information requests to nine data brokers to better understand their practices. The primary purpose of the upcoming report is to shine a light on the data broker industry and increase awareness about its practices.

- Telecheck and Certegy: The FTC aggressively enforces the Fair Credit Reporting Act (FCRA), which sets forth procedures governing some of the most important uses of Big Data – determining whether to give consumers credit, a job, or insurance. Recently the Commission obtained \$3.5 million penalties from TeleCheck and Certegy, two companies that advise merchants on whether to accept consumers’ checks, based on their past financial history. The complaints alleged that TeleCheck and Certegy violated the FCRA by failing to have appropriate procedures for consumers to dispute potential errors in their financial histories and failing to maintain the accuracy of the data provided to merchants. These types of violations can cause consumers to be denied the ability to write checks and obtain essential goods and services, like food and medicine.
- Data Security & Breach Notification Legislation: In recent testimony before Congress, the FTC reiterated its strong, bipartisan support for federal legislation that would (1) strengthen its existing authority governing data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach. Never has the need for legislation been greater. With reports of data breaches on the rise, and with a significant number of Americans suffering from identity theft, Congress needs to act.
- Other Legislative Proposals: In our 2012 Privacy Report, the Commission also called for general privacy legislation, as well as targeted legislation requiring data brokers to provide consumers with more transparency and choice about the data they hold about them. Although the current Commission has not weighed in on these legislative proposals, many of us at the Federal Trade Commission strongly support enactment of such legislation to protect consumers across the many contexts in which their data is collected, and level the playing field and provide clear rules of the road for businesses.
- Protecting vulnerable consumers and targeted groups – We have also made it a priority to stop fraudulent and deceptive practices targeted at particular groups of consumers, including Spanish-speaking consumers, seniors, and financially-distressed consumers. Some of our work in this space includes:
  - Senior Safe Alert: Earlier this year the FTC and the Florida Attorney General halted and froze the assets of an Orlando-based operation that used robocalls to pitch purportedly “free” medical alert devices to senior citizens by falsely representing that the devices had been purchased for them by a

relative or friend. The defendants also allegedly led consumers to believe that the devices were endorsed by various health organizations and that they would not be charged anything before the devices were activated. Many of the consumers who received the defendants' calls are elderly, live alone, and have limited or fixed incomes.

- Oro Marketing: Also, earlier this year, the Commission shut down Oro Marketing, a telemarketing operation that allegedly targeted Hispanic consumers with false promises that they could make money by reselling high-end goods such as Gucci and Ralph Lauren, and then charged them between \$400 and \$490 up-front for shoddy, off-brand products. We also alleged that the telemarketers threatened consumers who refused to pay with arrest and phony lawsuits, and made other intimidating statements.
- Prime Legal: In 2012, as part of the Distressed Homeowner Initiative, a multi-agency federal enforcement crackdown, the FTC charged eleven companies and five individuals with running an illegal mortgage relief scheme, which operated under various names, including Prime Legal Plans. Using a sham non-profit front, and a maze of other companies, the scheme reeled in consumers with false promises that enrollment would save their homes from foreclosure or result in lower mortgage payments. As part of Prime Legal's settlement with the FTC, the Commission obtained \$3.6 million in redress, and defendants were required to surrender their assets and were banned permanently from providing mortgage relief and debt relief services to consumers.
- COPPA: The Commission also continues to focus on providing strong safeguards for sensitive data, including information about children. For example, last year the FTC's final Children's Online Privacy Protection Act Rule went into effect. The new Rule responds to collection practices made possible by new technology – namely, data-gathering tools like social media and mobile applications – and gives parents greater control over the personal information that websites and online services may collect from children under 13.
- “Gatekeepers and Facilitators” – In addition to targeting fraudsters, we have made it a priority to target entities and practices that enable fraud and deception to occur – in other words, the “gatekeepers and facilitators.” Examples of our work in this area include:
  - Payment processors and lead generators: We have targeted payment

processors, lead generators, and others who knowingly facilitate fraud and deception. For example, in *Process America*, we alleged that the company used unfair tactics to open and maintain scores of merchant accounts for Infusion Media, which perpetrated the “Google Money Tree” work-at-home scheme. Using these scores of merchant accounts, Infusion Media charged more than \$15 million in unauthorized charges on consumers’ debit and credit card accounts. The complaint against Process America alleged that the defendants knew or should have known that they were processing charges that consumers had not authorized. Evidence that consumers were being charged without their permission included plainly deceptive statements on merchant websites, notices that the merchant should be placed in Visa and MasterCard chargeback monitoring programs, and chronically excessive chargeback rates.

- Telemarketing Sales Rule: We also have proposed amendments to the Telemarketing Sales Rule to prohibit use of certain payment methods typically used for fraud (*e.g.*, remotely-created checks). Specifically, the changes would stop telemarketers from dipping directly into consumer bank accounts by using unsigned checks and “payment orders” that have been “remotely created.” These instruments can make it easy for unscrupulous telemarketers to debit bank accounts without permission. The proposed changes would also bar telemarketers from getting paid with traditional “cash-to-cash” money transfers, as well as “cash reload” mechanisms, that scammers rely on to get money quickly and anonymously from consumer victims.
- Apple: Our recent settlement with mobile platform provider Apple is also a good example. Apple agreed to provide full refunds to consumers, paying a minimum of \$32.5 million, to settle FTC charges that the company billed consumers for millions of dollars of charges incurred by children in kids’ mobile apps without their parents’ consent. The complaint alleges that Apple violated the FTC Act by failing to tell parents that by entering a password they were approving a single in-app purchase and also 15 minutes of additional unlimited purchases their children could make without further action by the parent. In addition, according to the complaint, Apple has often presented a screen with a prompt for a parent to enter his or her password in a kids’ app without explaining to the account holder that password entry would finalize any purchase at all. Apple received at least tens of thousands of complaints about unauthorized in-app purchases by children, and consumers have reported millions of dollars in unauthorized charges to Apple.

- Thank you again for having me here today. I'm happy to take any questions.