Federal Trade Commission
2014 Privacy and Data Security Update[1]

The Federal Trade Commission (FTC or Commission) is an independent U.S. law enforcement agency charged with protecting consumers and enhancing competition across broad sectors of the economy. The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace. The FTC also has authority to enforce a variety of sector specific laws, including the Truth in Lending Act, the CAN-SPAM Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act. This broad authority allows the Commission to address a wide array of practices affecting consumers, including those that emerge with the development of new technologies and business models.

How Does the FTC Protect Consumer Privacy and Ensure Data Security?

The FTC uses a variety of tools to protect consumers' privacy and personal information. The FTC's principal tool is to bring enforcement actions to stop law violations and require companies to take affirmative steps to remediate the unlawful behavior. This includes, when appropriate, implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, disgorgement of ill-gotten gains, deletion of illegally obtained consumer information, and provision of robust notice and choice mechanisms to consumers. If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. The FTC can also obtain civil monetary penalties for violations of certain privacy statutes, including Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and Do Not Call. To date, the Commission has brought hundreds of privacy and data security cases protecting billions of consumers.

The FTC's other tools include conducting studies and issuing reports, hosting public workshops, developing educational materials for consumers and businesses, testifying before the U.S. Congress and commenting on legislative and regulatory proposals that affect consumer privacy, and working with international partners on global privacy and accountability issues.

In all of its privacy work, the FTC's goals have remained constant: to protect consumers' personal information and ensure that consumers have the confidence to take advantage of the many benefits offered in the marketplace.

---

1 This document covers the time period from approximately January 2014-December 2014. It will be updated on an annual basis. There is some overlap with previously issued Privacy and Data Security Update, which covered the time period from approximately January 2013-March 2014. *See* http://www.ftc.gov/reports/privacy-data-security-update-2013.

ENFORCEMENT

The FTC has unparalleled experience in consumer privacy enforcement. Its enforcement actions have addressed practices offline, online, and in the mobile environment. It has brought enforcement actions against well-known companies, such as Google, Facebook, Twitter, and Microsoft, as well as lesser-known companies. The FTC's consumer privacy enforcement orders do not just protect American consumers; rather, they protect consumers worldwide from unfair or deceptive practices by businesses within the FTC's jurisdiction.

General 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**. In 2014, the FTC announced the following privacy cases:

- The FTC charged Jerk, LLC d/b/a Jerk.com with harvesting personal information from Facebook to create profiles labeling people a "Jerk" or "not a Jerk," then falsely claiming that consumers could revise their online profiles by paying $30. According to the FTC's complaint, the defendants mislead consumers that the content on Jerk.com had been created by other Jerk.com users, when in fact most of it had been harvested from Facebook. The company also falsely led consumers to believe that by paying for a Jerk.com membership, they could access "premium" features that could allow them to change their "Jerk" profile. This matter is currently in litigation.

- Snapchat, Inc. settled charges that it deceived consumers with promises about the disappearing nature of messages sent through the service. Snapchat marketed the app's central feature as the user's ability to send snaps that would "disappear forever" after the sender-designated time period expired. Despite Snapchat's claims, the complaint describes several simple ways that recipients could save snaps indefinitely, such as by using third-party apps to log into the Snapchat service.

- In its case against TRUSTe, Inc., a major provider of privacy certifications for online businesses, the FTC alleged that from 2006 until January 2013, TRUSTe failed to conduct annual recertifications of companies holding TRUSTe privacy seals in over 1,000 incidences, despite representing on its website that companies holding TRUSTe Certified Privacy Seals receive recertification every year.

- An Atlanta-based health billing company and its former CEO settled FTC charges that they misled thousands of consumers who signed up for an online billing portal by failing to adequately inform them that the company would seek highly detailed medical information from pharmacies, medical labs, and insurance companies. PaymentsMD, LLC, and its former CEO, Michael C. Hughes, allegedly used the sign-up process for a "Patient Portal" – where consumers could view their billing history – as a pathway to deceptively seek consumers' consent to obtain detailed medical information about the consumers.

- A district court ordered the operators of several international tech support scams to pay more than $5.1 million in redress. In PCCare247, Inc., Virtual PC Solutions, Zeal IT Solutions Pvt Ltd., Lakshmi Infosoul Services Pvt Ltd., Pecon Software Ltd., and Finmaestros LLC, the defendants posed as major computer security and manufacturing companies to deceive consumers into believing that their computers were riddled with viruses, spyware and other malware. The complaints alleged that the defendants were not actually affiliated with major computer security or manufacturing companies and they had not detected

viruses, spyware or other security or performance issues on the consumers' computers. The defendants charged consumers hundreds of dollars to remotely access and "fix" the consumers' computers.

- In Innovative Marketing, Inc., a federal appeals court upheld a district court ruling that imposed a judgment of more than $163 million on an individual defendant for her role in an operation that used computer scareware to trick consumers into thinking their computers were infected with malicious software, and then sold them software to "fix" their non-existent problem.

- In cases against two massive telemarketing operations, the defendants allegedly used software designed to trick consumers into thinking there were problems with their computers, then subjected those consumers to high-pressure deceptive sales pitches for tech support products and services to fix their non-existent computer problems. The defendants allegedly defrauded tens of thousands of consumers out of more than $120 million by deceptively marketing computer software and tech support services. The first case was against defendants Inbound Call Experts, LLC, also d/b/a Advanced Tech Support; Advanced Tech Supportco, LLC; PC Vitalware, LLC; Super PC Support, LLC; Robert D. Deignan; Paul M. Herdsman; Justin M. Wright; PC Cleaner, Inc.; Netcom3 Global, Inc.; Netcom3, Inc., also d/b/a Netcom3 Software Inc.; and Cashier Myricks, Jr., also known as Cashier Myrick. The second case was against defendants Boost Software Inc. and Amit Mehta; and Vast Tech Support LLC, also d/b/a OMG Tech Help, OMG Total Protection, OMG Back Up, downloadsoftware.com, and softwaresupport.com; OMG Tech Help LLC; Success Capital LLC; Jon Paul Holdings LLC; Elliot Loewenstern; Jon-Paul Vasta; and Mark Donahue..

- The FTC obtained a federal court order to shut down Pairsys, Inc., a company that allegedly tricked seniors and other targeted populations into providing financial information to pay hundreds of dollars for technical support services they did not need, as well as software that was otherwise available for free.

- A federal court ordered Bayview Solutions to notify consumers that it posted their sensitive personal information online and explain how they can protect themselves against identity theft and other fraud. In the course of trying to sell debt portfolios, the debt seller posted more than 70,000 consumers' bank account and credit card numbers, birth dates, contact information, employers' names, and information about debts the consumers allegedly owed on a public website.

- The FTC obtained an injunction against debt seller Cornerstone and Company, LLC, to notify more than 70,000 consumers that it had posted their sensitive personal information online. The company, which was attempting to sell portfolios of past-due payday loan, credit card, and other purported debt, was also required to explain to consumers how to protect themselves in light of the disclosures.

- In its case against Caprice Marketing, the FTC stopped an operation that promised to help consumers get payday loans. The defendants allegedly used multiple websites to collect consumers' names, Social Security numbers, bank routing numbers, and bank account numbers. Instead of loans, the defendants used consumers' financial information to debit their bank accounts in increments of $30 without their authorization.

- The FTC obtained a court order halting an online payday lending scheme that allegedly cost consumers tens of millions of dollars. The FTC alleged that CWB Services, LLC used personal financial information bought from data brokers to make unauthorized deposits into consumers' bank accounts. After depositing money into consumers' accounts without their permission, the defendants withdrew bi-weekly reoccurring "finance charges" without any of the payments going toward reducing the loan's principal.

The defendants then contacted the consumers by phone and email, telling them that they had agreed to, and were obligated to pay for, the "loan" they never requested and misrepresented the true costs of the purported loans.

- According to the FTC's complaint, data broker LeapLab bought payday loan applications of financially strapped consumers, and then sold that information to marketers whom it knew had no legitimate need for it. These include: marketers that made unsolicited sales offers to consumers via email, text message, or telephone call; data brokers that aggregated and then resold consumer information; and phony internet merchants that used the information to withdraw millions of dollars from consumers' accounts without their authorization.

- An affiliate marketer, Jason Q. Cruz d/b/a Appidemic Inc., agreed to settle charges that he was responsible for sending millions of unwanted text messages to consumers that deceptively promised "free" gift cards and electronics. In its complaint, the FTC alleged that he sent spam text messages to consumers around the country offering free merchandise, such as $1,000 gift cards to major retailers or free iPads, to those who clicked on links in the messages.

- Twelve defendants that allegedly operated websites enticing consumers with bogus offers and hired affiliates to send spam text messages to promote them agreed to pay $2.5 million in settlements with the FTC. The defendants are: SubscriberBASE Holdings, Inc.; SubscriberBASE, Inc., Jeffrey French; All Square Marketing, LLC; Threadpoint, LLC; PC Global Investments, LLC; Slash 20, LLC; Brent Cranmer; PC Global Investments, LLC, and Slash 20, LLC; Christopher McVeigh; and Michael Mazzella. According to the complaint, the corporate defendants hired affiliate marketers to send millions of spam text messages to consumers around the country. When consumers clicked on the links in the spam text messages, they were taken to landing pages operated by one group of defendants that asked them to "register" for the free prizes they had been offered. The registration process was allegedly a method to collect information about the consumers that was then sold to third parties. Once consumers provided this information, they were taken to sites owned by another group of defendants. On these sites, consumers were told that to win the prize they had been offered, they were required to complete a number of "offers," many of which involved either paid subscriptions to services, or applying for credit.

- Rishab Verma and his company, Verma Holdings, LLC, agreed to settle charges that they were responsible for sending millions of spam messages to consumers across the country, which contained false promises of "free" $1,000 gift cards for major retailers like Walmart, Target and Best Buy. The settlement contains a monetary judgment of $2,863,000, which is suspended due to the defendants' inability to pay after Verma and the company pay $26,100.

- In CPA Tank, Inc., the company settled allegations that it paid affiliates to send out the spam text messages promoting supposedly "free" merchandise, such as $1,000 gift cards for Wal-Mart and Best Buy. People who clicked on the links in the text message did not receive the promised items, but instead were taken to websites that requested they provide personal information and sign up for numerous additional offers – often involving other purchases or paid subscriptions.

- The FTC's case against Advert Marketing, Inc., which includes a monetary judgment of $4.2 million, settles charges that the affiliate-marketing scammers sent millions of spam text messages to consumers across the U.S. with false promises of $1,000 gift cards to retailers like Best Buy, Target and Walmart.

Data Security

Since 2002, the FTC has brought over **50 cases** against companies that have engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk. In 2014, the FTC brought the following cases:

- In addition to privacy allegations against Snapchat, Inc., the FTC also alleged that the company deceived consumers over the amount of personal data it collected and the security measures taken to protect that data from misuse and unauthorized disclosure. In fact, the case alleges, Snapchat's failure to secure its Find Friends feature resulted in a security breach that enabled attackers to compile a database of 4.6 million Snapchat usernames and phone numbers.
- The FTC settled charges that Fandango, LLC misrepresented the security of its mobile app and failed to secure the transmission of millions of consumers' sensitive personal information from its mobile app. In particular, the app failed to authenticate and secure the connections used to transmit this data, and left consumers' credit card information vulnerable to exposure.
- Credit Karma, Inc. settled allegations that it failed to secure the transmission of consumers' sensitive personal information from its mobile app, including Social Security numbers, birthdates, and credit report information. The company also allegedly misrepresented the security of the app, which was vulnerable due to the failure to authenticate and secure the connections used to transmit consumer data.
- In its 50th data security settlement, the FTC settled allegations that GMR Transcription Services – an audio file transcription service – violated the FTC Act. According to the complaint, GMR relied on service providers and independent typists to transcribe files for their clients, which include healthcare providers. As a result of GMR's alleged failure to implement reasonable security measures and oversee its service providers, at least 15,000 files containing sensitive personal information – including consumers' names, birthdates, and medical histories – were available to anyone on the Internet.
- According to the FTC, GeneLink, Inc. and foru™ International Corp., the makers of genetically customized nutritional supplements, deceptively and unfairly claimed that they had reasonable security measures to safeguard and maintain personal information – including genetic information, Social Security numbers, bank account information, and credit card numbers.
- In 2012, the FTC filed suit against global hospitality company Wyndham Worldwide Corporation and three of its subsidiaries for alleged data security failures that led to three data breaches at Wyndham hotels in less than two years. In 2014, a federal district court affirmed the FTC's authority to challenge unfair data security practices using its Section 5 authority.
- The FTC sent a letter to Verizon closing an investigation into the company's shipment of routers set by default to an outdated encryption standard. As discussed in the letter, staff recommended closing the investigation based on Verizon's overall data security practices related to its routers, along with efforts by Verizon to mitigate the risk to its customers' information. Verizon took steps to mitigate the risk to consumer information by pulling the routers from its distribution centers, reaching out to customers with information about changing the encryption standard to the newer standard, and offering customers the ability to upgrade to new units.

Credit Reporting & Financial Privacy

The **Fair Credit Reporting Act (FCRA)** sets out rules for companies that use data to determine creditworthiness, insurance eligibility, suitability for employment, and to screen tenants. The FTC has brought **100 FCRA cases** against companies for credit-reporting problems and has collected **over $30 million in civil penalties**. The **Gramm-Leach-Bliley ("GLB") Act** requires financial institutions to send consumers annual privacy notices and allow them to opt out of sharing their information with unaffiliated third parties. It also requires financial institutions to implement reasonable security policies and procedures. Since 2005, the FTC has brought **almost 30 cases for violation of the GLB Act**. In 2014, the FTC brought the following cases:

- Data broker Instant Checkmate, Inc. agreed to settle FTC charges that it violated the FCRA by providing reports about consumers to users such as prospective employers and landlords without taking reasonable steps to make sure that they were accurate, or without making sure their users had a permissible reason to have them. The case imposes a $525,000 fine.
- A data broker, Infotrack Information Services, Inc., agreed to settle FTC charges that it violated the FCRA by failing to provide adverse action notices to consumers, as well as by providing reports about consumers to prospective employers and landlords without taking reasonable steps to make sure that they were accurate. InfoTrack and its owner agreed to pay a $1 million fine.
- TeleCheck Services, Inc., one of the nation's largest check authorization service companies, agreed to pay $3.5 million to settle claims that they violated the FCRA by failing to follow proper dispute procedures, including refusing to investigate certain disputes.

U.S.-EU Safe Harbor

The U.S.-EU Safe Harbor Framework provides a way for businesses to transfer personal data from the EU to the U.S. in a manner consistent with EU law. The U.S. Department of Commerce administers the voluntary framework, and the FTC provides an enforcement backstop. To participate, a company must self-certify annually to the Department of Commerce that it complies with the seven privacy principles required to meet the EU's adequacy standard: notice, choice, onward transfer, security, data integrity, access, and enforcement. The FTC is strongly committed to vigilant Safe Harbor enforcement. Since 2009, the FTC has used Section 5 to bring **24 Safe Harbor cases**. During the past year, the FTC brought the following cases:

- The FTC obtained separate settlements with fourteen businesses that allegedly falsely claimed to abide by the Safe Harbor. The companies settling with the FTC represented a cross-section of industries, including retail, professional sports, laboratory science, online gaming, data broker, debt collection, and information security. The FTC complaints charge each company with representing, through statements in their privacy policies or display of a Safe Harbor certification mark, that they held current Safe Harbor certifications, even though the companies had allowed their certifications to lapse. Under the proposed settlement agreement, each company is prohibited from misrepresenting the extent to which it participates in any privacy or data security program sponsored by the government or any other self-regulatory or standard-setting organization. The companies are:
    - Apperian, Inc., a company specializing in mobile applications for business enterprises and security;
    - Atlanta Falcons Football Club, LLC, a National Football League team;

- Baker Tilly Virchow Krause, LLP, an accounting firm;
- BitTorrent, Inc., a provider of peer-to-peer (P2P) file sharing protocol;
- Charles River Laboratories International, Inc., a global developer of early-stage drug discovery processes;
- DataMotion, Inc., a provider of platform for encrypted email and secure file transport;
- DDC Laboratories, Inc., a DNA testing lab and the world's largest paternity testing company;
- Level 3 Communications, LLC, one of the six largest ISPs in the world;
- PDB Sports, Ltd., d/b/a Denver Broncos Football Club, a National Football League team;
- Reynolds Consumer Products Inc., a maker of foil and other consumer products;
- Receivable Management Services Corporation, a global provider of accounts receivable, third-party recovery, bankruptcy and other services;
- Tennessee Football, Inc., a National Football League team;
- Fantage.com, the maker of a popular multiplayer online role-playing game directed at children ages 6-16; and
- American Apparel, a clothing manufacturer and retailer.

- The FTC's proposed order in the case against TRUSTe, Inc., a major provider of privacy certifications for online businesses, prohibits it from making misrepresentations about its certification process or timeline. While the FTC's case, discussed above, did not allege any Safe Harbor violations, the order applies to all of TRUSTe's certification programs, and explicitly includes its U.S.-EU Safe Harbor certification work.

Children's Privacy

The **Children's Online Privacy Protection Act of 1998 ("COPPA")** generally requires websites and apps to get parental consent before collecting personal information from children under 13. Since 2000, the FTC has brought **over 20 COPPA cases** and collected **millions of dollars in civil penalties**. In 2013, the FTC updated it regulatory rule that implements COPPA to address new developments – such as social networking, smartphone Internet access, and the ability to use geolocation information – that affect children's privacy. (The new rule went into effect July 1, 2013). During the past year, the Commission brought the following cases:

- The FTC's complaint against TinyCo, Inc. alleged that many of the company's popular apps, which were downloaded more than 34 million times across the major mobile app stores, targeted children. The company allegedly failed to follow the steps required under COPPA related to the collection of children's personal information, and agreed to pay a $300,000 civil penalty.
- Online review site Yelp, Inc., agreed to settle charges that, from 2009 to 2013, the company collected personal information from children through the Yelp app without first notifying parents and obtaining their consent. Under the terms of the settlement, Yelp must pay a $450,000 civil penalty.
- Following a public comment period, the FTC approved the kidSAFE Seal Program as a safe harbor program under COPPA. The COPPA safe harbor provision provides flexibility and promotes efficiency in

complying with the Act by encouraging industry members or groups to develop their own COPPA oversight programs.

- Following a public comment period and review of iVeriFly's proposed COPPA verifiable parental consent method application, the FTC determined it was unnecessary to approve the company's specific method. Under the COPPA Rule, online sites and services directed at children must obtain permission from a child's parents before collecting personal information from that child. The rule includes a provision allowing interested parties to submit new verifiable parental consent methods to the Commission for approval. The FTC determined that iVeriFly's proposed method – which relies on the use of Social Security numbers and knowledge-based authentication questions – is a variation on existing methods already recognized in the Rule, or recently approved by the Commission.

- The FTC sent a letter to BabyBus, a China-based developer of mobile applications directed to children, warning that the company may be in violation of the COPPA Rule. In the letter, the FTC notes that its child-directed applications appear to collect precise geolocation information about users without first obtaining parental consent. The letter calls on BabyBus to evaluate its apps and determine whether they may be in violation, and informed the company that the Commission will review the apps again in the next month to ensure compliance.

- Following a public comment period, the FTC denied AgeCheq, Inc's proposed verifiable parental consent method, because it incorporates methods already enumerated under the Rule.

Do Not Call

In 2003, the FTC amended the **Telemarketing Sales Rule** (TSR) to create a national Do Not Call (DNC) Registry, which now includes more than 217 million active registrations. Do Not Call provisions prohibit sellers and telemarketers from engaging in certain abusive practices that infringe on a consumer's right to be left alone, including calling an individual whose number is listed with the Do Not Call Registry or who has asked not to receive telemarking calls from a particular company. Since 2004, the FTC has brought **119 cases enforcing Do Not Call Provisions against telemarketers**. Through these enforcement actions, the Commission has sought civil penalties, monetary restitution for victims of telemarketing scams, and disgorgement of ill-gotten gains from the 369 companies and 292 individuals involved. Although a number of cases remain in litigation, the 103 cases that have concluded thus far have resulted in orders totaling **more than $130 million in civil penalties and $1 billion in redress or disgorgement**. During the past year, the Commission brought the following cases:

- In Worldwide Info Services, Inc., the FTC and the Office of the Florida Attorney General obtained a settlement to permanently stop an operation that used pre-recorded telephone calls, commonly known as 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 order includes a judgment of nearly $23 million, most of which will be suspended after the defendants surrender assets including cash, cars, and a boat.

- Versatile Marketing Solutions settled FTC allegations that the home security company illegally called millions of consumers on the DNC Registry to pitch home security systems. VMS bought phone numbers from lead generators, who had obtained the information by illegal means through rampant use of robocalls. VMS subsequently called these consumers without first checking to see if they had registered

their telephone numbers on the DNC Registry, and ignored warning signs that the lead generators were engaged in illegal telemarketing practices.

- The FTC obtained a temporary restraining order to shut down a medical discount scheme by AFD Advisors that scammed seniors across the U.S. by offering phony discounts on prescription drugs and pretending to be affiliated with Medicare, Social Security, or medical insurance providers. According to the FTC, the defendants violated Section 5 of the FTC Act by deceptively presenting themselves as government or insurance representatives, as well as by telling consumers that the discount plans they were selling could provide substantial discounts on prescription drugs. AFD also violated the TSR for their deceptive acts and for calling consumers whose numbers were on the DNC Registry.

- In IAB Marketing Associates, LP, the FTC settled allegations that defendants, who operated a bogus trade association, tricked consumers into buying phony health insurance through deceptive telemarketing, including through illegal robocalls and illegal calls to customers on the DNC Registry. The settlement bans the defendants from selling healthcare-related products and includes a $125 judgment that will be partially suspended once the defendants surrender assets valued at over $1 million, including $502,000 in IRA funds and personal property that includes five luxury cars.

- A federal district court barred Cuban Exchange, Inc., the operators of an illegal robocall scheme, from making illegal robocalls and calling consumers whose phone numbers are on the DNC Registry. The FTC alleged that the defendants "spoofed" the FTC's own toll-free number on consumers' caller ID and misled more than 13,000 people into believing the operation had a connection with the FTC and could help get refunds from the Commission.

- In Vacation Communications Group, the defendants allegedly called timeshare owners and claimed they had buyers willing to pay a specified price for their properties, or that the timeshares would be sold in a specified period of time. At most, after charging consumers' accounts, the defendants provided agreements to "advertise" consumers' timeshare units. In both cases, the defendants allegedly violated the TSR by calling consumer whose numbers were on the DNC Registry.

- The FTC charged that Centro Natural Corp. cold-called consumers and threatened them with harsh consequences, such as arrest, legal actions, and immigration status investigations, if they failed to make large payments on bogus debts. The defendants' telemarketers also pressured and deceived consumers into paying for unwanted products by telling consumers it would "settle" their debt. Centro also regularly cold-called consumers whose phone numbers were on the DNC Registry, and failed to pay fees for the DNC Registry.

- Educational services company WordSmart Corporation settled allegations that it deceptively marketed the company's programs to the parents of school-age children who wanted to improve their children's performance in school or help them prepare for standardized tests. In addition, the defendant allegedly repeatedly called consumers whose phone numbers were listed on the DNC Registry, refused to honor requests to stop calling, and failed to connect a consumer to a sales representative within two seconds after a consumer answered the phone, as required by the TSR.

- At the FTC's request, a federal court halted a telemarketing scheme that tricked senior citizens by pretending to be part of Medicare, and took millions of dollars from consumers' bank accounts without their consent. According to the complaint, Sun Bright Ventures LLC called consumers – including many whose numbers were listed on the DNC Registry – pretending to be affiliated with Medicare

and obtained consumers personal information, including bank account data. Sun Bright then debited consumers' bank accounts without providing a product or service.

- The FTC obtained orders against three deceptive timeshare resale operations, banning them from selling timeshare property resale services. The settlements with Vacation Communications Group, LLC, Resort Property Depot, Inc.; and Resort Solutions Trust, Inc. resolve charges that the companies violated the TSR and lured consumers into paying hefty up-front fees, falsely claiming they had prospective buyers for properties they wanted to sell.

- A federal appellate court upheld a district court ruling that several defendants based in the United States and Canada deceived consumers through a telemarketing scheme designed to sell them phony mortgage assistance and debt relief programs. E.M.A. Nationwide and several other defendants allegedly operated a call center in Montreal that cold-called thousands of U.S. consumers, including those whose numbers were registered on the DNC Registry, pitching programs that would supposedly help them pay, reduce, or restructure their mortgage and other debts.

- The FTC obtained a permanent ban from telemarketing and robocalling against Sonkei Communications, an operation that enabled telemarketers to make illegal robocalls, call phone numbers on the DNC Registry, and mask Caller ID information.

- A federal district court found Dish Network, LLC liable for tens of millions of DNC violations. The court determined that Dish is responsible not only for the calls it placed to numbers on the DNC Registry, but it is also liable for calls placed by others the company retained and authorized to market its products and services.

- In Direct Financial Management, Inc., the FTC reached a settlement with four of the defendants in an allegedly phony debt relief services operation that claimed that, for $995, it would dramatically reduce consumers' credit card interest rates. According to the complaint, the defendants called numbers on the DNC Registry and violated the TSR to target financially strapped consumers with fraudulent debt relief services.

- As part of a broader sweep, the FTC took action against Lanier Law, LLC, a mortgage relief operation that allegedly preyed on distressed homeowners by misrepresenting it could get a favorable loan modification, and illegally charging advance fees. The defendant violated the DNC Rule by calling consumers who were on the DNC Registry, and by failing to buy the DNC Registry in any state where they operated.

- In Acquinity Interactive LLC, et al., defendants paid approximately $10 million to settle charges that they violated the FTC Act and the TSR. According to the complaint, the defendants operated a massive scam that sent unwanted text messages to millions of consumers, many of whom later received illegal robocalls, phony "free" merchandise offers, and unauthorized charges crammed on their mobile phone bills.

- In First Consumers, the FTC shut down a multi-million dollar telemarketing fraud that targeted U.S. seniors across the nation, scamming tens of thousands of consumers in violation of the FTC Act and the TSR. Telemarketers who carried out the fraud allegedly impersonated government and bank officials, and enticed consumers to disclose their confidential bank account information to facilitate the fraud. The defendants then used that account information to create checks drawn on the consumers' bank accounts and deposit them into corporate accounts they established.

ADVOCACY

When courts, government offices, or other organizations consider cases or policy decisions that affect consumers or competition, the FTC may provide its expertise and advocate for policies that protect consumers and promote competition. In 2014, the FTC filed the following comments related to privacy issues:

- The FTC filed a comment with the National Highway Traffic Safety Administration (NHTSA) on a proposed initiative that would require all cars to have a vehicle-to-vehicle (V2V) communications system in place by 2019. The FTC's comment noted the significant safety benefits that could result from such systems being implemented and applauded NHTSA's approach to addressing privacy and security risks, such as by designing a V2V system to limit the data collected and stored to only that which serves its intended safety purpose.
- In a comment to the Department of Energy regarding its multistakeholder effort to develop a voluntary code of conduct for smart grid privacy and security, FTC staff commended the group's efforts to develop a code focused on the important principles of transparency, accountability, and consumer choice. Among other things, the staff emphasized the importance of providing privacy disclosures in a clear and conspicuous way, at a just-in-time point, rather than buried in an extensive privacy policy or terms of service.
- FTC staff filed a public comment with the National Telecommunications and Information Administration (NTIA) regarding how developments in "Big Data" affect consumer privacy and the interests reflected in the Administration's Consumer Privacy Bill of Rights. The comment describes FTC staff's support for de-identification, accountability mechanisms, and the "notice and consent" model as vital tools to protect consumer privacy in a Big Data era.

RULES

As directed by Congress, the FTC has authority to develop rules that regulate specific areas of consumer privacy and security. Since 2000, the FTC has promulgated rules in a number of these areas:

- The Health Breach Notification Rule requires certain Web-based businesses to notify consumers when the security of their electronic health information is breached.
- The Red Flags Rule requires financial institutions and certain creditors to have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.
- The COPPA Rule requires websites and apps to get parental consent before collecting personal information from kids under 13. The Rule was revised in 2013 to strengthen kids' privacy protections and gives parents greater control over the personal information that websites and online services may collect from children under 13.
- The GLB Privacy Rule sets forth when car dealerships must provide a consumer with a notice explaining the institution's privacy policies and practices and provide a consumer with an opportunity to opt out of, disclosures of certain information to nonaffiliated third parties.
- The GLB Safeguards Rule requires financial institutions over which the FTC has jurisdiction to develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards.
- The Telemarking Sales Rule requires telemarketers to make specific disclosures of material information; prohibits misrepresentations; limits the hours that telemarketers may call consumers; and sets payment restrictions for the sale of certain goods and services. Do Not Call provisions of the Rule prohibit sellers and telemarketers from engaging in certain abusive practices that infringe on a consumer's right to be left alone, including calling an individual whose number is listed with the Do Not Call Registry or who has asked not to receive telemarking calls from a particular company. The Rule also prohibits robocalls – prerecorded commercial telemarketing calls to consumers –unless the telemarketer has obtained permission in writing from consumers who want to receive such calls.
- The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Rule is designed to protect consumers from deceptive commercial email and requires companies to have opt out mechanisms in place.
- The Disposal Rule under the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), which amended the FCRA, requires that companies dispose of credit reports and information derived from them in a safe and secure manner.
- The Pre-screen Opt-out Rule under FACTA requires companies that send "prescreened" solicitations of credit or insurance to consumers to provide simple and easy-to-understand notices that explain consumers' right to opt out of receiving future offers.

WORKSHOPS

Beginning in 1996, the FTC has hosted over 35 workshops, town halls, and roundtables bringing together stakeholders to discuss emerging issues in consumer privacy and security. In 2014, the FTC hosted the following privacy events:

- The FTC held a workshop entitled *Big Data: A Tool for Inclusion or Exclusion?* to further explore the use of "big data" and its impact on American consumers, including low income and underserved consumers.
- The FTC hosted a three-part Spring Privacy Series to examine the privacy implications of three new areas of technology that have garnered considerable attention for both their potential benefits and the possible privacy concerns they raise for consumers.
    - The first event focused on the privacy and security implications of mobile device tracking, which involves tracking consumers in retail and other businesses using signals from their mobile devices.
    - The second seminar examined alternative scoring products, which are used for a variety of purposes, ranging from identity verification and fraud prevention to marketing and advertising. Because consumers are largely unaware of these scores, and have little to no access to the underlying data that comprises the scores, the event discussed the privacy concerns and questions raised by such predictive scores.
    - The final seminar examined consumers' use of connected health and fitness devices that regularly collect information about them and transmit this information to other entities

REPORTS AND SURVEYS

The FTC is a leader in developing policy recommendations related to consumer privacy and data security. The FTC has authored **over 50 reports**, based on independent research as well as workshop submissions and discussions, in a number of areas involving privacy and security. In 2014, the FTC released the following:

- The FTC issued *Data Brokers: A Call for Transparency and Accountability*. The report found that data brokers operate with a fundamental lack of transparency and recommended that Congress consider enacting legislation to make data broker practices more visible to consumers and to give consumers greater control over the their personal information.
- FTC staff issued a report examining mobile shopping apps. The report, *What's the Deal? An FTC Study on Mobile Shopping Apps*, looked at some of the most popular apps used by consumers to comparison shop, collect and redeem deals and discounts, and pay in-store with their mobile devices. It concluded, among other things, that such apps should more clearly describe how they collect, use, and share consumer data, as well as ensure that their data security promises translate into sound data security practices.

CONSUMER EDUCATION AND BUSINESS GUIDANCE

Educating businesses and consumers about privacy and security issues is critical to the FTC's mission. The Commission has distributed **millions of copies of educational materials** for consumers and businesses to address ongoing threats to security and privacy. The FTC has developed extensive materials providing guidance on a range of topics, such as identity theft, Internet safety for children, mobile privacy, credit reporting, behavioral advertising, peer-to-peer file sharing, Do Not Call, and computer security. Examples of such education and guidance materials released in 2014 include:

- The FTC released an updated version of Net Cetera: Chatting with Kids About Being Online, our guide to help parents and other adults talk to kids about being safe, secure, and responsible online. This new version deals with such topics as mobile apps, public Wi-Fi security, text message spam, and offers updated guidance on COPPA.
- For consumers who may have been affected by the recently-announced breaches at major retailers, the FTC posted information online about steps people should take to protect themselves.
- The Commission sponsors OnGuard Online, a website designed to educate consumers about basic computer security. This year, people viewed more than 5.4 million pages on OnGuard Online and its Spanish-language counterpart, Alerta en Línea.
- The FTC uses blog posts to alert consumers to potential privacy and data security harms, and offer tips to help them protect their information. The FTC posts to its Consumer Blog as well as to blogs to OnGuard Online and the sites for National Consumer Protection Week and Military Consumer. Some examples include: what people should know about web-cam hackers, including security features to look for in an Internet-protocol camera; how people can protect their sensitive health information; tips on how people can protect themselves if their data is exposed in a data breach; how people can remove malware and secure their computers; privacy threats in photo-sharing apps.
- The FTC also has a Business Center Blog that explains, in plain language, recent enforcement actions, reports, and guidance. Some examples of blogs about privacy and data security include: the announcement of GMR Transcription Services, the FTC's 50th data security settlement; steps that human resources professionals can take to protect sensitive consumer information; and highlights of the latest updates to the FTC's COPPA Rule FAQs.
- The FTC hosted 16 events across the country, along with a series of national webinars and Twitter chats as part of Tax Identity Theft Awareness Week. The events were designed to raise awareness about tax identity theft and provide consumers with tips on how to protect themselves, and what to do if they become victims.
- The FTC issued new business guidance about privacy and data security, including updated Frequently Asked Questions for COPPA Rule compliance, as well as guidance for employers conducting background checks.

INTERNATIONAL ENGAGEMENT

A key part of the FTC's privacy work is engaging with international partners. The agency works closely with foreign privacy authorities, international organizations, and global privacy networks to develop robust mutual enforcement cooperation on privacy and data security investigations and cases. The FTC also plays a lead role in advocating for strong, globally interoperable privacy protections for consumers around the world.

Enforcement Cooperation

The FTC cooperates on enforcement matters with its foreign counterparts through informal consultations, memoranda of understanding, complaint sharing, and statutory mechanisms developed pursuant to the U.S. SAFE WEB Act, which authorizes the FTC to share information with foreign law enforcement authorities and provide them with investigative assistance by using the agency's statutory powers to obtain evidence in appropriate cases. During 2014, the FTC took several steps to enhance privacy enforcement cooperation:

- In a Memorandum of Understanding with the United Kingdom's Information Commissioner's Office, the FTC and the U.K. authority agreed voluntarily to engage in mutual assistance and the exchange of information in connection with the enforcement of applicable privacy laws.
- The FTC participated in several initiatives of the Global Privacy Enforcement Network (GPEN). FTC staff continue to serve on the GPEN Committee. The FTC contributed to the second annual GPEN sweep, on app privacy practices in March 2014. In October 2014, the FTC participated in the GPEN workshop on the use of publicity as a regulatory compliance technique. In 2014, participation in GPEN increased to over 50 authorities.

Policy

The FTC advocates for sound policies that ensure strong privacy protections for consumer data that is transferred outside the U.S. and across other national borders. It also works to promote global interoperability among privacy regimes and better accountability from businesses involved in data transfers. During the past year, the FTC played a lead role in these international efforts:

- Through a Mapping Project involving privacy regulators and experts from the Asia Pacific Economic Cooperation (APEC), including the FTC and the European Union (EU), the FTC continued to contribute to international initiatives on consumer privacy protections for cross-border data flows. The project released a tool, called a "referential," which is designed to serve as a practical reference tool for companies that seek "double certification" under APEC and EU systems for cross-border data transfers. The FTC also continued its work on the implementation of APEC's Cross-Border Privacy Rules (CBPR) System, which was put into place in 2011. The FTC serves as an administrator of APEC's Cross-border Privacy Enforcement Arrangement, which now has 26 participating member authorities.
- Other international engagement included participation at the Asia-Pacific Privacy Authorities Forum, the International Conference of Data Protection and Privacy Commissioners, and the OECD.
- The FTC, together with the Department of Commerce and other U.S. agencies, also engaged bilaterally in negotiations over improvements to the U.S.-EU Safe Harbor Framework. In March 2014, the United States and the European Union pledged to strengthen the Safe Harbor Framework in a comprehensive

manner to "ensure data protection and enable trade through increased transparency, effective enforcement and legal certainty when data is transferred for commercial purposes." The FTC brought several Safe Harbor enforcement actions, described in detail above.