Privacy & Data Security
Update: 2017

Federal Trade Commission
January 2017 - December 2017

Federal Trade Commission 2017 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 Promote 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 providing robust transparency 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 and rules, including the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, and the Telemarketing Sales Rule. 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 of products offered in the marketplace.

[1] This document covers the time period from January 2017-December 2017. It will be updated on an annual basis.

ENFORCEMENT

The FTC has unparalleled experience in consumer privacy enforcement. The Commission has brought over 500 enforcement actions protecting the privacy of consumer information. 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 focuses on protecting American consumers, but the orders the FTC obtains in its cases also protect consumers worldwide from unfair or deceptive practices by businesses within the FTC's jurisdiction.

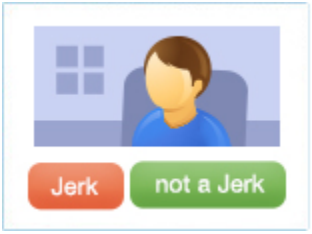
General Privacy

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 50 general privacy lawsuits**. In 2017, the FTC announced the following privacy cases:

- The FTC and 32 State Attorneys General alleged that Lenovo, one of the world's largest computer manufacturers, began selling consumer laptops in the United States in August 2014 that came with a preinstalled software program called VisualDiscovery that interfered with how a user's browser interacted with websites. According to the complaint, VisualDiscovery software – developed by a company called Superfish – delivered pop-up ads from the company's retail partners whenever a user's cursor hovered over a similar looking product on a website. To deliver its ads, VisualDiscovery acted as a "man-in-the-middle" between consumers' browsers and the websites they visited, even sensitive encrypted websites. Without the consumer's knowledge or consent, the FTC alleged that this "man-in-the-middle" technique allowed VisualDiscovery to access all of a consumer's sensitive personal information transmitted over the Internet, including login credentials, Social Security numbers, medical information, and financial and payment information. The FTC alleged, among other things, that Lenovo's failure to disclose that VisualDiscovery acted as a man-in-the-middle between consumers and all the websites with which they communicated, including sensitive encrypted websites, and collected and transmitted consumer Internet browsing data to Superfish, was both an unfair and deceptive practice.
- Ride-sharing company Uber Technologies, Inc. settled FTC charges that it deceived consumers by, among other things, failing to live up to its claims that it closely monitored employee access to consumer and driver data. According to the complaint, in the wake of news reports alleging Uber employees were improperly accessing consumer data, the company issued a statement that it had a "strict policy prohibiting" employees from accessing rider and driver data – except for a limited set of legitimate business purposes – and that employee access would be closely monitored on an ongoing basis. In December 2014, Uber developed an automated system for monitoring employee access to consumer personal information, but the company stopped using it less than a year after it was put in place. The FTC's complaint alleges that Uber, for more than nine months afterwards, rarely monitored internal access to personal information about users and drivers. Under the proposed consent agreement, Uber agreed to implement a comprehensive privacy program and obtain regular, independent audits.

- The FTC alleged that Blue Global, a lead generation business, misled consumers into filling out loan applications and sold those applications – including consumers' sensitive data – to virtually anyone willing to pay for the leads. The complaint alleges that Blue Global operated dozens of websites that offered services to consumers seeking a variety of loans, including payday and auto loans. The company claimed it would search a network of 100 or more lenders, and connect each loan applicant to the lender that would offer them the best terms. The FTC charged that, in reality, the defendants: sold very few of the loan applications to lenders; did not match applications based on loan rates or terms; and sold the loan applications to the first buyer willing to pay for them. The company also promised to protect and secure the sensitive information consumers provided, such as Social Security numbers and bank account numbers, claiming the information was only provided to "trusted lending partners." The FTC alleges, however, that the company provided the complete loan application data submitted by consumers to any potential buyer without conditions and with little regard to how it would be used. The complaint further alleges that this sensitive personal and financial information was shared and sold indiscriminately without consumers' knowledge or consent.
- A membership reward service called Upromise, aimed at consumers trying to save for college, paid a $500,000 civil penalty to settle allegations that it violated a 2012 FTC order. Following the 2012 order, Upromise encouraged consumers to download a toolbar called "RewardU." The FTC's order required Upromise to clearly and prominently disclose RewardU's data collection and use, and to obtain third-party assessments and certifications of the toolbar describing specific safeguards and their effectiveness in protecting consumers' personal information. The Commission alleged that Upromise failed to comply with both provisions of the order.
- VIZIO, Inc., one of the world's largest manufacturers and sellers of internet-connected "smart" televisions, agreed to pay $2.2 million to settle charges by the FTC and the New Jersey Attorney General that it installed software on its TVs to collect viewing data on 11 million consumer TVs without consumers' knowledge or consent. According to the agencies' complaint, VIZIO manufactured smart TVs that capture second-by-second information about video displayed on the smart TV, and appended specific demographic information to the viewing data, such as sex, age, income, and marital status. VIZIO then allegedly sold this information to third parties, who used it for various purposes, including targeting advertising to consumers across devices. The complaint alleges that VIZIO's data tracking – which occurred without viewers' informed consent – was unfair and deceptive, in violation of the FTC Act and New Jersey consumer protection laws.
- In SQ Capital, the FTC obtained a $4.1 million judgment and a ban on handling certain sensitive financial information about consumer debts against an operation that sold lists of fake payday loan debts to debt collectors. The complaint alleged that the defendants sold lists of fake payday loan debts containing information about millions of consumers, which debt collectors then used to demand payment. The lists had extensive personal information, including Social Security and bank account numbers. As a result, consumers were harassed for debts they did not owe, and in some cases paid the fake debts.
- The FTC filed a complaint, alleging that ACDI Group purchased a portfolio of more than 2,000 supposedly past-due payday loans. Although the debts were allegedly fake, the names, addresses, Social Security numbers, telephone numbers, and email addresses attached to them were real. The defendants allegedly used this personal information to collect the phony debts and continued to collect on those debts, even after learning the debts were fake and receiving a full refund for their debt portfolio purchase.

- The FTC and Illinois Attorney General obtained a ban against Stark Law – the operators of a fake debt collection scheme – from the debt collection business and from selling debt portfolios, and required them to surrender assets totaling at least $9 million, which will be returned to consumers. The orders also prohibit them from misrepresenting financial products and services, profiting from customers' personal information collected as part of the challenged practices, and failing to dispose of such information properly. According to the complaint, since at least 2011, the defendants targeted consumers who obtained or applied for payday or other short-term loans, pressuring them into paying debts they either did not owe or that the defendants had no authority to collect. The defendants allegedly called consumers and demanded immediate payment for supposedly delinquent loans, often armed with consumers' sensitive personal and financial information.
- The FTC approved a final order with mobile ad network Turn Inc., which allegedly deceived consumers by falsely leading them to believe they could reduce the extent to which the company tracked them online and on their mobile phones. According to the FTC's complaint, Turn told consumers that they could choose not to be tracked by deleting cookies or changing device settings. Despite this, in 2013 Turn joined a Verizon Wireless program in which the carrier added unique identifiers to its users' mobile internet traffic, which allegedly allowed Turn to track millions of Verizon Wireless devices and recreate the cookies on those devices even after an owner deleted them or reset the identifier on their device. In addition, the agency charged that Turn's opt-out mechanism only applied to mobile browsers, and did not block tailored, anonymous ads on mobile applications.
- The Commission modified the compliance monitoring provision of its order against the operators of Jerk.com in response to a First Circuit decision affirming the Commission's finding of liability and sustaining all other aspects of the Commission's remedial order. The Commission found that the operators of Jerk.com, a website that billed itself as "the anti-social network," misled consumers by claiming that content on the website was posted by other users. Instead, most of the content came from Facebook profiles mined by the operators. The Commission also found that the defendants misrepresented the benefits of a paid membership which, for $30, purportedly allowed consumers to update information in their Jerk.com profiles. In fact, consumers who paid for the membership were unable to correct information about them on the site, and did not receive anything of value for their "membership."



Data Security

Since 2002, the FTC has brought over **60 cases** against companies that have engaged in unfair or deceptive practices that that failed to adequately protect consumers' personal data. Significant developments in 2017 included the following:

- Uber Technologies, Inc., described above, also allegedly deceived consumers by failing to reasonably secure sensitive consumer data stored in the cloud. The FTC's complaint alleges that despite Uber's claim that data was "securely stored within our databases," Uber's security practices failed to provide reasonable security to prevent unauthorized access to consumers' personal information in databases Uber stored with a third-party cloud provider. For example, according to the complaint, Uber did not require engineers and programmers to use distinct access keys to access personal information stored

in the cloud. Instead, Uber allowed them to use a single key that gave them full administrative access to all the data, and did not require multi-factor authentication for accessing the data. In addition, Uber stored sensitive consumer information, including geolocation information, in plain readable text in database back-ups stored in the cloud. As a result, an intruder accessed personal information about Uber drivers in May 2014, including more than 100,000 names and driver's license numbers that Uber stored in a datastore operated by Amazon Web Services.

- As discussed above, the FTC and 32 State Attorneys General alleged that Lenovo sold hundreds of thousands of laptops with a preinstalled "man-in-the-middle" software program called VisualDiscovery that, among other things, created serious security vulnerabilities. To facilitate its display of pop-up ads on encrypted websites, the complaint alleged that VisualDiscovery used an insecure method to replace digital certificates for those websites with its own VisualDiscovery-signed certificates. Digital certificates are used to signal to a user's browser that the encrypted websites visited by a consumer are authentic and not imposters. VisualDiscovery, however, did not adequately verify that the websites' digital certificates were valid before replacing them, and used the same, easy-to-crack password on all affected laptops rather than using unique passwords for each laptop. Because of these security vulnerabilities, consumers' browsers could not warn users when they visited potentially spoofed or malicious websites with invalid digital certificates. The vulnerabilities also could allow potential attackers to intercept consumers' electronic communications with any website, including financial institutions and medical providers, by simply cracking the pre-installed password. The complaint alleges that Lenovo did not discover these security vulnerabilities because it failed to assess and address security risks created by third-party software it preloaded on its laptops.
- The FTC filed a complaint against computer networking equipment manufacturer D-Link, alleging that inadequate security measures taken by the company left its wireless routers and Internet cameras vulnerable to hackers. According to the complaint, D-Link promoted the security of its routers on the company's website, but the company failed to take steps to address well-known and easily preventable security flaws. Litigation in this matter is ongoing.

Credit Reporting & Financial Privacy

The **Fair Credit Reporting Act (FCRA)** sets out requirements for companies that use data to determine creditworthiness, insurance eligibility, suitability for employment, and to screen tenants. The FTC has brought **over 100 cases** against companies for violating the FCRA and has collected **over $30 million in civil penalties**. The **Gramm-Leach-Bliley ("GLB") Act** requires financial institutions to send consumers initial and 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 violations of the GLB Act**. In 2017, the FTC brought the following case:

- The FTC alleged that online tax preparation service TaxSlayer violated the Gramm-Leach-Bliley Act's Safeguards Rule, which requires financial institutions to implement safeguards to protect customer information, and the Privacy Rule and Regulation P, which requires financial institutions to deliver privacy notices to customers. The FTC alleged that TaxSlayer violated the Safeguards Rule by failing: to develop a written comprehensive security program until November 2015; to conduct a risk assessment to identify reasonably foreseeable internal and external risks to security; and to implement information security safeguards that would help prevent a cyberattack. For example, TaxSlayer failed to implement adequate risk-based authentication measures that would have helped reduce the

chances of an attack from hackers who had used stolen credentials to try to gain access to TaxSlayer customer accounts, according to the complaint. The FTC also alleged that the company did not require consumers to choose strong passwords, exposing customers to the risk that attackers could guess commonly used passwords to access their TaxSlayer accounts. The FTC alleged that malicious hackers were able to gain full access to nearly 9,000 TaxSlayer accounts between October 2015 and December 2015 and use that information to engage in tax identity theft, which allowed them to obtain tax refunds by filing fraudulent tax returns, according to the complaint. The FTC also alleged that the company violated the Privacy Rule and Regulation P by failing to provide its customers with a clear and conspicuous initial privacy notice and to deliver it in a way that ensured that customers received it.

International Enforcement

The FTC enforces key international privacy frameworks, including the EU-U.S. Privacy Shield Framework and the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CPBR) System.

The EU-U.S. Privacy Shield Framework provides a legal mechanism for companies to transfer personal consumer data from the European Union to the United States. This Framework, administered by the Department of Commerce, protects consumers' privacy and security through an agreed set of Privacy Shield Principles. The FTC plays a significant role in enforcing companies' privacy promises as violations of Section 5 of the FTC Act. This year, the FTC brought its first three enforcement actions under the Privacy Shield, and participated in the first Annual Review of the framework, which became operational in August 2016. The FTC also affirmed its commitment to enforce a third data transfer mechanism, the Swiss-U.S. Privacy Shield Framework, which is modeled on the EU-U.S. Privacy Shield.

The FTC also serves as a privacy enforcement authority in the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CPBR) system. The APEC CBPR system is a voluntary, enforceable code of conduct designed to enhance the privacy and security of consumers' personal information transferred among the United States and other APEC members. Under the system, participating companies can be certified as compliant with APEC CBPR program requirements that implement APEC's nine data privacy principles.

Carrying out its enforcement role under these international privacy frameworks the FTC has brought 46 actions – 39 under an older "U.S.-EU" Safe Harbor program, 4 under APEC CBPR, and 3 under Privacy Shield. During the past year, the FTC brought the following cases:

- Three U.S. companies settled charges that they misled consumers about their participation in the European Union-United States Privacy Shield framework. According to the FTC, printing services company Tru Communication, human resources software company Decusoft, and Md7, which manages real estate leases for wireless companies, violated the FTC Act by falsely claiming that they were certified to participate in the EU-US Privacy Shield. The FTC also alleged that Decusoft falsely claimed participation in the Swiss-U.S. Privacy Shield framework. All three companies allegedly failed to complete the certification process for the Privacy Shield.
- The FTC approved final orders with three companies resolving allegations that they deceived consumers by misrepresenting their participation in the APEC CBPR system. In separate complaints, the FTC charged that Sentinel Labs, which provides endpoint protection software to enterprise customers, SpyChatter, the marketer of a private message app, and Vir2us, which distributes cyber security

software, falsely represented in their online privacy policies that they participated in the APEC CBPR system. Sentinel Labs also falsely claimed that it was a participant in a TRUSTe privacy program, according to the FTC.

Children's Privacy

The **Children's Online Privacy Protection Act of 1998 ("COPPA")** generally requires websites and apps to obtain verifiable 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 its 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. During the past year, the Commission took the following actions:

- In a new policy enforcement statement, the FTC provided additional guidance on how the COPPA Rule applies to the collection of audio voice recordings. The COPPA Rule requires websites and online services directed at children to obtain verifiable parental consent before collecting an audio recording, raising questions about the application of this requirement when a child's voice is collected for the sole purpose of instructing a command or request on Internet-connected devices. Under the policy enforcement statement, the FTC agreed not to take action against an operator for not obtaining verifiable parental consent before collecting the audio file with a child's voice when it is collected solely as a replacement of written words, such as to perform a search or to fulfill a verbal instruction or request, as long as it is held for a brief time.
- The FTC approved TRUSTe's proposed modifications to its safe harbor program under the COPPA Rule. The FTC's COPPA Rule includes a "safe harbor" provision that allows industry groups and others to seek Commission approval of self-regulatory guidelines that implement "the same or greater protections for children" as those contained in the COPPA Rule. Companies and organizations that participate in an FTC-approved safe harbor program will, in most circumstances, be subject to the review and disciplinary procedures provided in the safe harbor's guidelines in lieu of formal FTC investigation and law enforcement. After reviewing public comments, the FTC approved the proposed changes to TRUSTe's existing safe harbor program, including the addition of a new requirement that participants conduct an annual internal assessment of third-parties' collection of personal information from children on their websites or online services.

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 229 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, calling consumers after they have asked not to be called again, and using robocalls to contact consumers to sell goods or services. Since 2003, the FTC has brought **134 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 436 companies and 353 individuals involved. The 125 cases that

have concluded thus far have resulted in orders totaling **over $1.5 billion in civil penalties, redress, or disgorgement**. During the past year, the Commission initiated actions and settled or obtained judgments as described below:

- As the result of DNC litigation brought by the Department of Justice on behalf of the FTC, as well as the states of California, Illinois, North Carolina, and Ohio, a federal court ordered penalties totaling $280 million and strong injunctive relief against satellite television provider Dish Network. The court found Dish liable for millions of calls that violated the FTC's Telemarketing Sales Rule – including DNC, entity-specific, and abandoned-call violations – the Telephone Consumer Protection Act (TCPA), and state law. The civil penalty award included $168 million penalty for federal violations, which is a record in a DNC case. The remaining penalties were awarded to the states. Dish has appealed the district court's order.
- As part of Operation Game of Loans, the first coordinated federal-state law enforcement initiative targeting deceptive student loan debt relief scams, the FTC filed a complaint against A1 DocPrep, alleging that the defendants took at least $6 million from consumers through unlawful student loan debt relief and mortgage assistance relief schemes. According to the complaint, the defendants called consumers whose phone numbers were listed on the DNC Registry, claimed to be from the Department of Education, and promised to reduce borrowers' monthly payments or forgive their loans. The FTC also alleges the defendants targeted distressed homeowners, making false promises to consumers that they would provide mortgage relief and prevent foreclosure.
- The FTC filed a lawsuit against Student Debt Relief Group as part of Operation Game of Loans for taking at least $7.3 million from consumers struggling to repay their student loans. According to the complaint, the defendants contacted consumers whose phone numbers were listed on the DNC Registry, falsely claimed to be affiliated with the Department of Education, deceived consumers into paying up to $1,000 in illegal upfront fees to enter them into free government programs, and charged consumers monthly fees they claimed would be credited toward their student loans. In reality, the FTC alleged, defendants pocketed consumers' money and responded to mounting consumer complaints by changing their names rather than their business practices. The FTC also asserts that the defendants deceived consumers into providing them with Social Security numbers and Federal Student Aid identification information, allowing the defendants to hijack consumers' accounts while cutting them off from their loan servicers and the Department of Education.
- The FTC obtained a settlement order with Justin Ramsey, the ringleader of telemarketing operations that blasted illegal robocalls to consumers and called phone numbers listed on the DNC Registry. The order bans Ramsey and his company, Prime Marketing LLC from placing robocalls to individuals to sell goods or services, initiating sales calls to numbers listed on the DNC Registry, and selling data lists containing phone numbers listed on the Registry. Ramsey and Prime Marketing also agreed to a $2.2 million civil penalty, suspended upon payment of $65,000. The full judgment will become due if they are later found to have misrepresented their financial condition. According to the FTC's complaint, in 2012 and 2013 Ramsey and several co-defendants illegally blasted millions of robocalls to consumers and also placed millions of calls to phone numbers listed on the DNC Registry. In just one week in July 2012, the complaint states, the defendants made more than 1.3 million illegal robocalls to consumers nationwide, 80 percent of which were to numbers listed on the DNC Registry.

- A federal court approved default judgments against Aaron Michael Jones and nine companies whom the FTC charged with running an operation that blasted consumers with billions of illegal telemarketing robocalls. The FTC estimates that in making the illegal robocalls, Jones and the companies he controlled called numbers listed on the DNC Registry at a rate of more than 100 million per year. The court orders permanently ban Jones and the companies from all telemarketing activities, including initiating robocalls, calling numbers on the DNC Registry, and selling data lists containing consumers' phone numbers and other information. The order also imposes a $2.7 million penalty against Jones.
- The FTC obtained a final order against ABC Hispana Inc., which used telemarketers in Peru that allegedly employed deceptive and abusive tactics to sell products for learning English to Spanish-speaking consumers throughout the United States. The defendants sold booklets, CDs, DVDs, tablets and a Spanish-English dictionary, and threatened to sue, arrest or jail consumers, or seize their homes, if they did not pay. They pretended to be affiliated with the government, centro de ayuda (non-governmental "help center"), well-known companies such as Walmart, or a Spanish-language radio station. Among other things, the order imposes a judgment of more than $6.3 million and bans the defendants from telemarketing.
- As a result of DNC litigation brought on the FTC's behalf by the Department of Justice, KFJ Marketing Inc. entered into a settlement order imposing a $1.4 million civil penalty, suspended upon payment of $155,000. According to the complaint, the KFJ Marketing defendants placed millions of illegal robocalls generating leads for solar installation companies. The defendants' robocalls made statements such as: "This is an urgent call about your energy bill," and "stop the 14% increase coming soon." Consumers were told to press "1" to lower their electric bill. Those who did were transferred to a telemarketer who asked if they were also interested in solar panels. The final order also bans the owner of KFJ Marketing and his companies from engaging in telemarketing.
- The FTC filed an action against Higher Goals Marketing LLC to halt an alleged debt-relief scam that has defrauded numerous consumers struggling with credit card debt. The complaint alleges that the Higher Goals Marketing defendants used illegal robocalls, including calls to numbers on the DNC registry, to contact consumers, pitching their fake debt-relief services and charging hefty advance fees. Defendants guaranteed that consumers would substantially and permanently lower their credit card interest rates, and would save thousands of dollars in interest payments. In reality, the complaint alleges, the defendants were unable to deliver the promised results to most consumers. The Commission also alleges that several defendants previously worked for a nearly identical telemarketing operation shut down by court order in 2016 at the request of the FTC. These defendants set up a new operation selling similar bogus credit-card interest-rate-reduction services within weeks of the court order shuttering the earlier operation.
- The FTC and ten state partners obtained a stipulated final order against the remaining defendants in the Caribbean Cruise Line (CCL) robocall action that bars the defendants from initiating robocalls, helping anyone else make robocalls, and engaging in illegal telemarketing practices. The order also includes a judgment of $1.35 million, suspended after payment of $2,500. The complaint alleges that the CCL robocall campaign ran from October 2011 through July 2012 and averaged approximately 12 to 15 million illegal sales calls a day, including calls to numbers on the DNC registry. Consumers who answered these calls typically heard a pre-recorded message telling them they had been selected to participate in a 30-second research survey, after which they would receive a "free" two-day cruise to the Bahamas. In reality, the calls were designed to market CCL's cruises and various up-sell packages.

- In the Advertising Strategies LLC action, the FTC obtained a stipulated final order against operators of an alleged telemarketing scheme that pitched bogus online investment opportunities, defrauded consumers out of millions of dollars, and, in the process, illegally called consumers with phone numbers on the DNC Registry. The stipulated final order imposes a $25 million judgment, partially suspended upon the defendants' surrender of assets, which totaled approximately $7.7 million. The order also bars all defendants from telemarketing, marketing investment opportunities, and selling or otherwise benefiting from consumers' personal information.
- The FTC and the Florida Attorney General obtained stipulated final orders against defendants that bombarded consumers with illegal robocalls, including calls to numbers on the DNC registry, from "Card Member Services," pitching worthless credit card interest rate reduction programs in the All US Marketing LLC action. The complaint alleges that the defendants claimed to be from "credit card services" and "card member services" and charged consumers up to $4,999 for their non-existent services. The orders include permanently bans on robocalling (for defendants that engaged in robocalling), telemarketing, and providing debt relief services. The stipulated orders included suspended monetary judgments for various amounts; the largest suspended judgments reflected the total consumer harm in the case — $4.89 million.

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 2017, the FTC filed the following comments related to privacy issues:

- FTC staff filed a comment with the Federal Communications Commission (FCC) supporting that agency's proposal to restore FTC jurisdiction related to broadband Internet access services. The comment emphasized the FTC's strong track record of protecting consumer privacy and data security in various sectors, including across the Internet ecosystem, and described the FTC's expertise in protecting consumers from other kinds of harm, such as fraudulent business practices, deceptive advertising claims, and other types of deceptive or unfair practices. The comment noted that having one agency with jurisdiction over the entire Internet ecosystem will help ensure consistent standards and consistent application of those standards.
- FTC staff filed a comment with the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) on a draft template, developed by a diverse group of stakeholders, designed to be used by industry participants to communicate their policies on disclosing security vulnerabilities. In its comment on the template, staff noted that the FTC also has addressed the issue of vulnerability disclosure in its data security guidance, policy reports and through its business education campaigns. Staff also said that while the draft template is aimed at safety-critical industries, such as automobile and medical device manufacturers, the template could be a useful tool for any company providing software-based products and services to consumers. Staff recommended that the introduction to the draft template be revised to make clear that the recommendations could apply to more than just safety-critical industries. Staff further noted that companies that provide Internet-connected products or collect sensitive consumer information should consider implementing a vulnerability disclosure policy and related processes.
- The FTC filed a comment with a working group convened by the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) that is developing guidance about ways for Internet (IoT) device manufacturers to better inform consumers about security updates related to the devices. The FTC comments pertain to draft guidance on "key elements" that manufacturers should consider conveying to consumers to help them make better informed purchasing and use decisions. The Commission recommended certain modifications to the working group's "key elements" such as disclosing a minimum amount of time that consumers can expect security support for their product. Among the other suggested changes, the Commission recommended that manufacturers consider telling consumers upfront if a "smart" device will lose basic functionality after security support ends, provided that consumers would expect a similar "dumb" device to have a longer support lifespan. The FTC also recommended changes to the "additional elements" section in the guidance such as considering adoption of a uniform method for notifying consumers about updates that are not made automatically and considering providing real-time notification to consumers when manufacturers stop providing security updates for IoT devices.

- The Commission provided testimony to Congress on the role of antitrust enforcement in the debate over network neutrality. The testimony described the FCC's 2015 decision reclassifying broadband

Internet access service from a Title I information service to a Title II common carrier service and described how that decision removed the provision of broadband internet access service from FTC jurisdiction. The testimony also described the FCC's subsequent proposal to reverse that decision and FTC staff's comment on that proposal. The testimony also notes that while the debate has centered on the FCC, the FTC has expertise in the antitrust and consumer protection issues raised by net neutrality concerns.

- The FTC testified to Congress on the agency's commitment to protecting consumers and educating small businesses on ways to keep consumer data secure. The testimony highlighted the FTC's history of data security-related work, and described the FTC's extensive efforts to educate business and consumers on data security through advisories, published guides, videos, and workshops.

RULES

As directed by Congress, the FTC has authority to issue 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 consumers with initial and annual notices explaining the dealer'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. In 2017, the FTC reviewed public comments it received on the Rule as part of its systemic review of all current FTC rules and guides.
- 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 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. Following a public comment period as part of its systemic review of all current FTC rules and guides, in 2017 the FTC determined that it would reissue the Disposal Rule without change.
- 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 50** workshops, town halls, and roundtables bringing together stakeholders to discuss emerging issues in consumer privacy and security. In 2017, the FTC hosted the following privacy events:

- In January, the Commission hosted its second annual PrivacyCon, a conference to examine cutting-edge research and trends in protecting consumer privacy and security. The event brought together leading stakeholders, including whitehat researchers, academics, industry representatives, federal policymakers, and consumer advocates. PrivacyCon 2017 explored research focused on the Internet of Things and Big Data, mobile privacy, consumer privacy expectations, online behavioral advertising, and information security.
- The FTC's second FinTech Forum focused on two evolving types of financial technology: peer-to-peer payment systems and crowdfunding platforms. The FinTech Forum series is part of the FTC's ongoing work to protect consumers taking advantage of new and emerging financial technology. The forum examined the various models of crowdfunding and peer-to-peer payments used by companies, the potential benefits to consumers, and possible consumer protection concerns. In addition, the forum looked at how existing consumer protection laws might apply to crowdfunding and peer-to-peer payments.
- The FTC's third FinTech Forum examined the consumer implications of artificial intelligence and blockchain. The half-day event brought together industry participants, consumer groups, researchers, and government representatives, to examine the ways in which these technologies are being used to offer consumers services, the potential benefits, and consumer protection implications of these technologies.
- The FTC held a conference – Identity Theft: Planning for the Future – to examine the changing nature of identity theft and the challenges it poses. The conference gathered input from academics, business and industry representatives, government experts and consumer advocates to take a comprehensive look at how identity theft has evolved over the last decade and what we can do to address the challenges it poses.
- The FTC hosted a joint workshop with the National Highway Traffic Safety Administration ("NHTSA") entitled Connected Cars: Privacy, Security Issues Related to Connected, Automated Vehicles. The workshop brought together a variety of stakeholders, including industry representatives, consumer advocates, academics, and government regulators, to examine the consumer privacy and security issues posed by automated and connected motor vehicles.
- The FTC and Department of Education ("ED") held a joint workshop to examine Student Privacy and Ed Tech. While the growing use of technologies in the classroom has tremendous potential, this transformation in Ed Tech has raised questions about how the COPPA Rule applies in the school context, and how the Rule intersects with the Family Educational Rights and Privacy Act ("FERPA"). The workshop gathered information from stakeholders to help clarify how the FTC and ED can ensure that student privacy is properly protected without interfering with the promise of Ed Tech.

- In December, the FTC hosted its Informational Injury Workshop to examine consumer injury in the context of privacy and data security. Information about consumers has become a key input to innovation in products and services, yet consumers may suffer injury when information about them is misused. The workshop convened stakeholders to address questions such as how to best characterize these injuries, how to accurately measure such injuries and their prevalence, and what factors consumers consider when evaluating the tradeoffs between providing information and potentially increasing their exposure to injuries.

REPORTS AND SURVEYS

The FTC is a leader in developing policy recommendations related to consumer privacy and data security. The FTC has authored **approximately 60 reports**, based on independent research as well as workshop submissions and discussions, involving privacy and security. In 2017, the FTC released the following:

- The FTC held the IoT Home Inspector Challenge to encourage developers to create an innovative tool to help protect consumers from security vulnerabilities in the software of home devices connected to the Internet of Things. The winner of the $25,000 challenge proposed a mobile app, IoT Watchdog, that would enable users with limited technical expertise to scan their home Wi-Fi and Bluetooth networks to identify and inventory connected devices. It would flag devices with out-of-date software and other common vulnerabilities and provide instructions on how to update each device's software and fix other vulnerabilities.
- In January, the FTC released Cross-Device Tracking: An FTC Staff Report that describes the technology used to track consumers across multiple Internet-connected devices, the benefits and challenges associated with it, and industry efforts to address those challenges. The report made recommendations to industry about how to apply traditional principles like transparency, choice, and security to this relatively new practice.
- The FTC issued a staff perspective finding that most major online businesses are using proper email authentication technology to prevent phishing emails, but few of these businesses are taking full advantage of the latest technologies to combat phishing. The study found that most of the major online businesses it studied used Sender Policy Framework (SPF), an email authentication technology that enables Internet Service Providers to determine whether messages that claim to be from the businesses' email addresses actually come from the businesses. Fewer than 10 percent of those businesses, however, implemented a supplemental technology known as Domain Message Authentication Reporting & Conformance (DMARC) in a manner which would allow the businesses to receive intelligence on potential spoofing attempts and to instruct ISPs to automatically reject any unauthenticated messages that claimed to be from the businesses' email addresses. The staff perspective noted that by using DMARC to instruct receiving ISPs to reject unauthenticated messages, online businesses could further combat phishing by keeping these scam emails from showing up in consumers' inboxes.
- At the FTC's identity theft conference held in May, Commission staff presented research tracking the use of leaked consumer data. Staff created a decoy database of plausible but fake sensitive consumer information – names, addresses, phone numbers, email, and payment information – and posted it twice on a paste site frequented by identity thieves. The research demonstrated that identity thieves obtained the information in some cases in a matter of minutes, used IP addresses from close to 30 different countries, and attempted to make $12,825.53 in illegal purchases.

CONSUMER EDUCATION AND BUSINESS GUIDANCE

Educating businesses and consumers about privacy and data security issues – and how to address related threats – 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, Do Not Call, and computer security. Examples of such education and guidance materials released in 2017 include:

- The FTC launched its Stick with Security blog series, which expanded on the FTC's Start with Security business guidance. *Stick with Security* offers additional insight into the ten *Start with Security* principles based on the lessons of recent law enforcement actions, closed investigations, and experiences of companies.
- In May, the FTC launched a new site for small business owners. It includes educational materials to help small businesses stay ahead of the latest scams, reduce the risks from cyber threats, keep customer data safe and respond in case of a data breach.
- The Commission hosted small business owners in a series of public roundtables to discuss the challenges small businesses face in protecting the security of their computers and networks. The Engage, Connect, and Protect Initiative: Small Business and Data Security Roundtables brought together FTC staff along with the Small Business Administration and other federal partners, industry associations, and the small business communities in Cleveland, Des Moines, Charlotte, Dover, and Portland, Oregon. The comments and feedback generated by the roundtables will be used to help the FTC and its partners provide additional education and guidance for small businesses on cybersecurity issues.

- The FTC produced five new videos to help businesses with data protection. These videos covered topics such as how the NIST Cybersecurity Framework aligns with the FTC's work on data security, how to respond if your business is impersonated in a phishing scam, how businesses can defend against ransomware, using email authentication to prevent phishing emails from getting through to your customers, and steps companies should take to respond to a data breach.
- The FTC held a series of events as part of Tax Identity Theft Week to alert consumers, tax professionals, veterans, and small businesses to ways they can minimize their risk of tax identity theft, and recover if it happens. The FTC joined the IRS, the Department of Veterans Affairs, the AARP Fraud Watch Network, and other organizations to discuss tax identity theft, IRS imposter scams, cybersecurity and identity theft recovery.
- The FTC revised its Six-Step Compliance Plan for Your Business to provide additional guidance for businesses about complying with COPPA. The updated materials reflect developments in the marketplace, such as the introduction of Internet-connected toys and other devices for kids, voice-activated products that collect personal information, and newly-approved methods for obtaining verifiable parental consent.
- The FTC's Consumer Blog alerts consumers to potential privacy and data security hazards and offers tips to help them protect their information. In 2017, the most-read consumer blog posts addressed the

Equifax breach and how to respond. The FTC published a series of posts about the breach, credit freezes, fraud alerts, and an Equifax-related scam. To make it easier for people to find information related to the data breach, the FTC created a page that links to Equifax related blog posts, as well as articles about fraud alerts, credit freezes, and active duty alerts for service members, and information about what to do for consumers whose information was exposed.

- The FTC's Business Blog addresses recent enforcement actions, reports, and guidance. The privacy and data security posts written and most read in 2017 addressed topics including television viewing data collected without customer knowledge, FCRA requirements for background screening reports, fraud alerts and credit freezes, and COPPA compliance.
- The FTC also hosts a Technology Blog to discuss some of the more technical aspects of the agency's work. For example, last year the FTC posted a blog encouraging researchers to conduct research relevant to consumer protection and share it with the FTC.

INTERNATIONAL ENGAGEMENT

A key part of the FTC's privacy and security work is engaging with international partners. The agency works closely with foreign privacy authorities, international organizations, and global privacy authority networks to develop robust mutual enforcement cooperation on privacy and data security investigations. 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 mechanisms developed pursuant to the U.S. SAFE WEB Act, which authorizes the FTC, in appropriate cases, to share information with foreign law enforcement authorities and to provide them with investigative assistance using the agency's statutory evidence-gathering powers. Significant enforcement cooperation developments in 2017 include:

- The International Conference of Data Protection and Privacy Commissioners (ICDPPC), the premier global forum for privacy authorities, gave the FTC and its Australian and Canadian counterparts its "Grand Award for Innovation" for the agencies' collaboration in investigating the massive Ashley Madison data breach, which affected consumers in nearly 50 countries. At the end of 2016, the FTC entered into a court settlement with the Toronto-based operators of the adult dating website, which required them to implement a comprehensive data-security program and pay $1.6 million to settle charges that they deceived consumers and failed to protect 36 million users' account and profile information. The Australian and Canadian data protection authorities also reached their own settlements with the company and contributed to the FTC's investigation. In bestowing the award, the ICDPPC cited the three agencies' cooperation as a "model on how to achieve cross-border cooperation in privacy enforcement." The ICDPPC also gave the FTC and its collaborators the top award for "Dispute Resolution, Compliance and Enforcement."
- As part of its work on the management committee of the Global Privacy Enforcement Network (GPEN), the FTC helped to organize a first-ever GPEN enforcement workshop, which focused on building investigative and enforcement skills for privacy enforcement authorities. During 2017, GPEN grew to include 66 authorities from 49 countries, with over 340 staff from participating agencies registered on an internal GPEN discussion forum.
- To further enforcement cooperation with EU data protection authorities (DPAs) under the Privacy Shield framework, the FTC took on several implementation initiatives including, participating in the annual review of the program, identifying a dedicated liaison to assist with DPAs' inquiries regarding Privacy Shield participants' compliance with the Privacy Shield Principles, and finalizing a standard DPA referral form.

Policy

The FTC advocates for sound policies that ensure strong privacy protections for consumer data transferred across 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, in addition to participating, alongside the Department of Commerce and other U.S. agencies, in the First Annual Review of the new EU-U.S. Privacy Shield Framework for transatlantic data transfers, the FTC played a leading role in policy deliberations and projects on privacy and data security internationally:

- The FTC participated in the International Conference of Data Protection and Privacy Commissioner's (ICDPPC) Group of Experts on Legal and Practical Solutions for Cooperation, developing key principles for legislation that facilitates greater enforcement cooperation, which were endorsed at the 39th conference in Hong Kong.
- The FTC participated in meetings and activities of the APEC Electronic Commerce Steering Group, the Asia-Pacific Privacy Authorities Forum; the International Working Group on Data Protection in Telecommunications, and the OECD.

The FTC also engaged directly with numerous counterparts on privacy and data security issues including by hosting delegations and engaging in bilateral discussions with officials from the Canada, China, Japan, Korea, Singapore and the UK, as well as members of the Canadian Parliament and the European Parliament.

Additionally the FTC conducted technical cooperation missions on privacy and cross-border data transfer issues in Colombia and the Philippines. The agency also hosted an official from the European Data Protection Supervisor's office as part of its International Fellows Program.

As demonstrated above, the FTC was very active in protecting consumer privacy and data security in 2017. The FTC's prior work – in 2017 and long before – has prepared and positioned the agency to continue to be the leading U.S. agency on privacy and data security.

Federal Trade Commission
ftc.gov