

Privacy & Data Security **Update: 2018**

Federal Trade Commission
January 2018 - December 2018



Federal Trade Commission 2018 Privacy and Data Security Update¹

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, the Telemarketing Sales Rule, the Fair Debt Collection Practices Act, and the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act. To date, the Commission has brought hundreds of privacy and data security cases.

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 and data security work, the FTC's goals have remained constant: to protect consumers' personal information; and to 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 2018-December 2018. It will be re-issued on an annual basis.

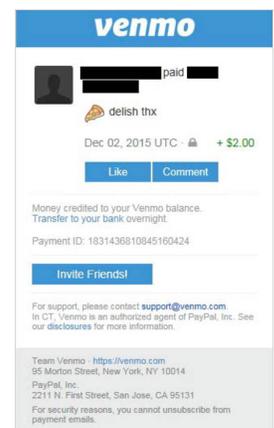
ENFORCEMENT

The FTC has deep experience in consumer privacy enforcement. The Commission has brought hundreds of 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 **75 general privacy lawsuits**. In 2018, the FTC announced the following privacy cases:

- ▶ The FTC and the state of Nevada obtained a final court order shutting down revenge porn website [MyEx.com](#) and requiring the operators to pay more than \$2 million. The FTC and Nevada alleged that MyEx.com solicited intimate pictures and videos of victims, along with personal information such as their names, addresses, employers, and social media account information. In numerous instances, defendants allegedly charged victims fees from \$499 to \$2,800 to remove their images and information from the site. In addition to shutting down the website and ordering monetary relief, the order also bans defendants from posting intimate images and personal information in their possession, requires the defendants to destroy all such images and information in their possession, and prohibits them from charging individuals fees for removing such content from a website. The order further requires third parties to disable any website hosted for the defendants when those third parties have knowledge that the site posts revenge porn.
- ▶ The FTC entered into a settlement with PayPal, Inc. over, among other things, allegedly deceptive privacy settings in its peer-to-peer payment service, [Venmo](#). The complaint alleged that Venmo misrepresented what steps were necessary to keep financial transactions private. The complaint also alleged that Venmo did not satisfy the Gramm-Leach-Bliley Privacy Rule and Safeguards Rule requirements. The settlement prohibits Venmo from misrepresenting the extent of control provided by any of its privacy settings and requires it to make affirmative disclosures about its privacy practices.
- ▶ The FTC alleged that mobile phone manufacturer [BLU Products, Inc.](#) and its co-owner allowed a China-based third-party service provider to collect detailed personal information about consumers, such as text message contents, which the service provider did not need, and which were contrary to promises BLU made to consumers. As part of the settlement, defendants must implement a comprehensive data security program to help prevent unauthorized access to consumers’ personal information and address security risks related to BLU phones. In addition, BLU will be subject to third-party assessments of its security program every two years for 20 years.
- ▶ The FTC charged [Sun Key Publishing, Inc.](#) and [Fanmail.com](#) with using deceptive tactics to obtain consumers’ personal information to sell as marketing leads for post-secondary education programs. The complaint alleged that defendants targeted consumers interested in military service by operating imposter military recruiting websites such as army.com, armyenlist.com, and navyenlist.com in order



to induce consumers to provide their information online. The complaint further alleged defendants promised consumers that the information submitted on the imposter recruiting sites would not be shared with anyone else. Consumers who submitted their information received phone calls from the operation's telemarketers, who continued to pose as the military. The FTC obtained an order halting the deceptive practices and imposing more than \$12 million in civil penalties, which defendants satisfied by turning over several of the military-related domain names used to deceive consumers.

- ▶ In [Mobile Money Code](#), the FTC obtained stipulated final orders against defendants that contacted consumers through deceptive spam emails and then bilked them out of millions of dollars by falsely promising they could earn hundreds to thousands of dollars a day using defendants' Mobile Money Code products. In reality, these products were nothing more than generic software applications that could help the user create mobile-friendly websites. The stipulated final orders impose a \$7 million judgment, suspended upon the defendants' payment of \$698,500, which will be used to refund consumers defrauded by defendants' scheme. The orders also bar defendants from using any consumer information they collected as part of the scheme.
- ▶ In [Alliance Law Group](#), the Commission shut down an operation it alleged was collecting fake debts by posing as lawyers and falsely threatening to sue or have consumers arrested, and obtained a judgment of more than \$700,000. Defendants' collectors claimed to possess consumers' private information—including Social Security numbers, bank account numbers, or the names and contact information of relatives—to convince consumers that the calls were legitimate collection efforts and that consumers must pay the purportedly delinquent debts.
- ▶ The FTC shut down the fake debt collection scheme in [Lombardo, Daniels & Moss](#). The Commission alleged that defendants used intimidation and deception to collect more than \$2.1 million from consumers in allegedly delinquent payday loans or other debts. The Commission alleged that defendants obtained consumers' private financial information and then used it to convince consumers they were legitimate collectors calling about legitimate debts. The final orders prohibit defendants from buying or selling debt, profiting from customers' personal information collected as part of the challenged practices, and failing to dispose of such information properly.
- ▶ In [Hylan Asset Management, LLC](#), the FTC and the New York Attorney General's Office charged two operations and their principals with running a scheme to collect money from consumers on fake and unauthorized debts. According to the FTC, defendants bought, placed for collection, and sold lists of phantom debts, including debts that were fabricated by the defendants or disputed by consumers. The Commission alleged that the defendants obtained consumers' private financial information and then used it to convince consumers they were legitimate collectors calling about legitimate debts. Much of the phantom debt was purchased from individuals who previously had been banned from selling debt portfolios or from handling sensitive financial information about consumer debts.
- ▶ The FTC announced a nonpublic investigation into the privacy practices of Facebook, following press reports that the company may have shared consumer information with Cambridge Analytica, in violation of [Facebook's](#) consent decree with the FTC.

Data Security and Identity Theft

Since 2002, the FTC has brought **65 cases** against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data. Significant developments in 2018 included the following:

- ▶ [Uber Technologies, Inc.](#) agreed to an expanded settlement arising from a 2016 data breach. The FTC [previously announced](#) a proposed privacy and data security settlement against Uber in 2017. Following that announcement, the Commission learned that Uber had failed to disclose a significant breach of consumer data that occurred in the midst of the FTC's investigation that led to the 2017 settlement announcement. Due to Uber's misconduct related to the 2016 breach, Uber is now subject to additional requirements. Among other things, the revised settlement subjects Uber to civil penalties if it fails to notify the FTC of certain future incidents involving unauthorized access of consumer information.
- ▶ In its complaint against mobile phone manufacturer [BLU Products, Inc.](#) and its co-owner, discussed above, the FTC also alleged that defendants falsely claimed that they had implemented "appropriate" physical, electronic, and managerial procedures to protect consumers' personal information. In fact, according to the complaint, defendants failed to implement appropriate security procedures to oversee the security practices of their service providers. As a result, software preinstalled on BLU devices contained common security vulnerabilities that could enable attackers to gain full access to the devices.
- ▶ The FTC's complaint related to [Venmo](#), discussed above, also alleged that the company misrepresented the extent of security it provided to consumer financial accounts, claiming that it utilized "bank-grade security systems." The FTC alleged that Venmo did not have a written information security program through at least August 2014, and that, until at least March 2015, Venmo failed to notify users when their password or email address had been changed, or when a new device had been added to their account. As a result, unauthorized users were able to withdraw funds from consumer accounts – without Venmo notifying consumers. In addition, Venmo lacked adequate customer support to respond to consumer complaints about these incidents.
- ▶ As part of a sweep aimed at stopping the sale of fake documents that are used to commit identity theft and other frauds, the FTC alleged that [Katrina Moore](#), [Steven Simmons](#), [George Jiri Strnad](#), and their associated businesses, engaged in unfair practices by selling fake but authentic-looking documents, such as pay stubs, tax returns, and bank statements. According to the complaint, Moore's website also offered falsification services, promising to edit real bank statements and similar documents with fake information. Strnad's websites allegedly offered fake job verification services, enabling fraudsters to use fake jobs to apply for loans. The FTC settlements prohibit defendants from selling fake documents or any service for making fake documents, and require defendants to disgorge their ill-gotten gains.
- ▶ [VTech Electronics Limited](#) and its U.S. subsidiary agreed to settle charges that they failed to use reasonable and appropriate data security measures to protect personal information. The FTC alleged that defendants failed to implement adequate safeguards, such as implementing an intrusion detection or prevention system, to protect the personal information it collected through its Kid Connect mobile app. As a result, a hacker was able to access its computer network and the personal information of its users, including children. The FTC also alleged that VTech violated the FTC Act by falsely stating that most personal information submitted by users through its Learning Lodge and Planet VTech platforms would be encrypted, when in fact the company failed to encrypt any of this data. As part of the settlement, defendants agreed to implement a comprehensive data security program and obtain independent biennial audits for 20 years.

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 2018, the FTC brought the following cases:

- ▶ [RealPage, Inc.](#) agreed to pay a \$3 million civil penalty to settle FTC charges that it violated the FCRA by failing to take reasonable steps to ensure the accuracy of tenant screening information that it provided to landlords and property managers. The complaint alleged that from at least January 2012 until September 2017, RealPage used broad criteria to match applicants to criminal records, only applied limited filters to the results, and did not have policies or procedures in place to assess the accuracy of those results. The FTC alleged that RealPage's screening reports associated some potential renters with criminal records that did not belong to them and that those renters may have been turned down for housing or other opportunities. In addition to the civil penalty, the settlement also requires RealPage to maintain reasonable procedures to assure the maximum possible accuracy of the information it includes about individuals in its consumer reports.
- ▶ In June, a federal court ordered [Credit Bureau Center](#) and its owner to pay more than \$5.2 million to resolve FTC charges that they deceived consumers with fake rental property ads and deceptive promises of "free" credit reports, and then tricked consumers into enrolling into a costly monthly credit monitoring service. Many consumers did not realize they were enrolled until they noticed unexpected charges on their bank or credit card statements, sometimes after several billing cycles.
- ▶ In [Lending Club](#), the FTC filed a complaint alleging, among other things, that the company failed to deliver privacy notices required by the GLB Act's Privacy Rule and Regulation P. The FTC's complaint charges that Lending Club violated these Rules by failing to provide its customers with a clear and conspicuous initial privacy notice before collecting customers' financial data and by failing to deliver the notice in a way that ensured that customers received it. Instead, in order for customers to reach the privacy notice, customers had to click on a link to the Terms of Use policy, and then further find a link to Lending Club's privacy policy.
- ▶ The FTC filed a complaint and motion for preliminary injunction in federal district court alleging that [Alliance Security Inc.](#), a home security installation company, and its founder obtained hundreds of thousands of consumer credit reports without consumers' knowledge or permission and in violation of the FCRA.
- ▶ The FTC's settlement related to peer-to-peer payment service [Venmo](#), discussed above, also alleged that the company did not satisfy the GLB Privacy Rule and Safeguards Rule requirements. The complaint alleged that Venmo did not satisfy the Privacy Rule requirement to deliver annual privacy notices to consumers. The Commission also alleged that Venmo violated the Safeguards Rule, which requires financial institutions to implement safeguards to protect the security, confidentiality, and integrity of customer information.

International Enforcement

The FTC enforces key international privacy frameworks, including the EU-U.S. Privacy Shield Framework and the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules System. It also enforces the Swiss-U.S. Privacy Shield Framework, which is modeled on the EU-U.S. Privacy Shield.

The [EU-U.S. Privacy Shield Framework](#) provides a legal mechanism for companies to transfer personal 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 participated, alongside the Department of Commerce and other U.S. government agencies, in the second [Annual Review](#) of the Framework, which became operational in August 2016.

The FTC also serves as a privacy enforcement authority in the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CBPR) 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 **51 actions – 39 under an older “[U.S.-EU Safe Harbor](#)” program, 4 under APEC CBPR, and 8 under Privacy Shield.**

During the past year, the FTC brought the following cases:

- ▶ Five U.S. companies settled charges that they misled consumers about their participation in the EU-U.S. Privacy Shield Framework. According to the FTC, [ReadyTech](#) falsely claimed on its website that it was in the process of certifying its compliance with the Framework, when it had not completed the steps necessary to participate. The FTC also alleged that [IDmission](#) falsely claimed to comply with the Framework, when in fact it too had never completed the necessary steps for certification. The FTC alleged that [SmartStart](#), [VenPath](#), and [mResource](#) each included statements on their websites that they participated in the Privacy Shield Framework, when, in fact, they had allowed their certifications to lapse.

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 **25 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 the Commission's case against [VTech Electronics Limited](#) and its U.S. subsidiary, discussed above, the FTC alleged that defendants collected personal information from hundreds of thousands of children and failed to provide notice of their information practices or obtain verifiable parental consent. Defendants also failed to use reasonable and appropriate data security measures to protect children's personal information, as required under COPPA. As part of the settlement, in addition to the relief described above, defendants agreed to a \$650,000 civil penalty.
- ▶ The FTC's complaint against talent search company [Explore Talent](#) alleged that the company had actual knowledge it collected personal information from more than 100,000 children under age 13, and

it failed to provide notice to parents about its information practices or to obtain verifiable parental consent. To settle charges that it violated COPPA, Explore Talent agreed to pay a \$235,000 civil penalty.

- ▶ The FTC sent warning letters to China-based [Gator Group Co., Ltd.](#) and Sweden-based [Tinitell, Inc.](#), notifying them that smart watches marketed for use by U.S. children must comply with COPPA. The FTC's letters noted that a review of their services showed that the companies did not appear to provide notice of their collection practices or to seek verifiable parental consent before collecting, using, or disclosing personal information from children, including geolocation information.
- ▶ The FTC approved the [Entertainment Software Ratings Board \(ESRB\) 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 ESRB's existing safe harbor program.

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 **235 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 DNC 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 **140 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 465 companies and 374 individuals involved. The 126 cases that have concluded thus far have resulted in orders totaling **over \$1.5 billion in civil penalties, redress, or disgorgement, and actual collections exceeding \$121 million**. During the past year, the Commission initiated actions and settled or obtained judgments as described below:

- ▶ The FTC sued a dietary supplement enterprise, [Redwood Scientific Technologies](#), which used illegal robocalls to deceptively market dissolvable oral film strips as effective smoking cessation, weight-loss, and sexual-performance aids. The FTC alleges that these products did not live up to defendants' claims, and that defendants violated the TSR through their use of harassing robocalls. The court granted the FTC's motion to temporarily halt the operation's marketing of these products. Litigation is ongoing.
- ▶ In the [Sunkey Publishing](#) action, discussed above, defendants operated imposter military recruiting websites, such as army.com and navyenlist.com, and agreed to settle charges that they targeted people seeking to join the armed forces and tricked them by falsely claiming to be affiliated with the military in order to generate sales leads for post-secondary schools. The agency alleged that defendants violated the Do Not Call provisions of the TSR by placing hundreds of thousands of illegal telemarketing calls to phone numbers on the DNC Registry and by failing to pay required fees.
- ▶ The FTC charged [Travis Deloy Peterson](#) with using fake veterans' charities and illegal robocalls to get consumers to donate things of significant value, which he then sold for his own benefit. Peterson allegedly made millions of robocalls asking people to donate automobiles, watercraft, real estate, and timeshares. The robocalls falsely claimed that these donations would go to veterans charities and were tax deductible. The Commission has charged Peterson with violating the FTC Act and the TSR. At the

FTC’s request, a federal court issued a temporary restraining order prohibiting Peterson from making unlawful robocalls or engaging in misrepresentations about charitable donations while the FTC’s enforcement action is proceeding.

- ▶ The FTC obtained temporary restraining orders and preliminary injunctions against 16 defendants—including recidivist robocallers Aaron Michael Jones and Justin Ramsey—who operated [Pointbreak Media](#), a Florida-based robocall scheme that deceived small business owners by falsely claiming to represent Google and falsely threatening that businesses would be removed from Google search results. The FTC’s complaint alleged that defendants have no relationship with Google, and yet they barraged consumers with robocalls threatening that Google will label their business “permanently closed” unless they “press one” to speak with a “Google specialist.” Defendants told those who responded that, for a purported one-time fee ranging from \$300 to \$700, they could “claim and verify” their Google listing and have unique “keywords” so their business would appear prominently when people search for their products or services. The complaint also alleges that while indiscriminately blasting their robocall messages to potential victims of their scam, the defendants also called individuals with numbers listed on the DNC Registry, in violation of the TSR.



- ▶ In [FTC v. James Christiano](#), the FTC filed a lawsuit against two related operations and their principals who allegedly facilitated billions of illegal robocalls to consumers nationwide, pitching everything from auto warranties to home security systems and purported debt-relief services. One set of defendants allegedly provided a computer-based telephone dialing platform that was used to blast out billions of robocalls and hundreds of millions of calls to numbers listed on the DNC Registry. The complaint alleges that the other set of defendants operated a call center in Guatemala that paid for the robocalls and received transfers of calls after consumers pressed “1” in response to the robocalls. The court has approved a settlement with one set of defendants.
- ▶ As discussed above, the FTC filed a complaint and motion for preliminary injunction in federal district court alleging that [Alliance Security Inc.](#), a home security installation company, and its founder, directly and through its authorized telemarketers, called millions of consumers whose numbers are on the DNC Registry. According to the FTC’s complaint, two of Alliance’s authorized telemarketers and their principals have agreed to settle charges that they made illegal calls on Alliance’s behalf. One of these telemarketers agreed to a complete ban on all telemarketing, and the other telemarketer agreed to a ban on the sale of any home security systems. Thus far, through these settlements, the FTC has obtained judgments totaling more than \$5.5 million.
- ▶ The FTC obtained a temporary restraining order and preliminary injunction to shut down robocallers operating as [Higher Goals Marketing LLC](#), who perpetrated an alleged credit card interest-rate reduction scam that deceived numerous consumers struggling with credit card debt. The complaint alleged that the individuals charged in this case, who previously worked for a nearly identical telemarketing operation shut down by court order in 2016 at the FTC’s request, 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 charged that [A1 DocPrep](#) used illegal calls to numbers listed on the DNC Registry to solicit sales connected to unlawful student loan debt relief and mortgage assistance relief schemes. According to the complaint, defendants impersonated the Department of Education and falsely promised to reduce borrowers' monthly payments or forgive their loans. The FTC also alleges defendants targeted distressed homeowners, making false promises to consumers that they would provide mortgage relief and prevent foreclosure. The court approved a settlement in which defendants agreed to a judgment of more than \$9.1 million.
- ▶ The FTC charged that M&T Financial Group and American Counseling Center Corp., doing business as, among other names, [Student Debt Relief Group](#), and their principal Salar Tahour, bilked consumers who were struggling to repay their student loans. According to the complaint, defendants 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 name rather than their business practices. The FTC also asserts that defendants violated the TSR by placing sales calls to numbers listed on the DNC Registry. The court approved a settlement in which defendants agreed to a judgment of more than \$11.6 million.
- ▶ The Commission charged the operators of a timeshare reselling scheme, known as [J. William Enterprises](#), with bilking at least \$15 million dollars from timeshare property owners by imposing hefty up-front fees based on false promises that they would sell or rent their properties. According to the FTC's complaint, defendants called timeshare property owners and falsely claimed that they had a buyer or renter willing to buy or rent their properties for a specified price, or they promised to sell the timeshares quickly, sometimes within a specified time period. Many of the defendants' telemarketing calls included illegal calls to consumers with numbers listed on the DNC Registry. The FTC reached a settlement in which defendants agreed to a judgment of more than \$18.7 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 2018, the FTC filed the following comments related to privacy issues:

- ▶ Staff [submitted a response](#) to the Consumer Product Safety Commission as part of the agency's [Request for Comments](#) on potential safety issues and hazards associated with Internet-connected consumer products. The comment emphasized that poor security in Internet of Things (IoT) devices might create technology-related hazards associated with the loss of critical safety function, loss of connectivity, or degradation of data integrity. For example, a car's braking system might fail if infected with malware, or carbon monoxide or fire detectors could stop working if they lose their Internet connection. The comment also outlined the FTC's education and enforcement work related to device and information security, particularly as it relates to IoT. As explained in the comment, the FTC previously has provided IoT manufacturers with [guidance](#) on how to predict and mitigate against privacy and security risks.
- ▶ FTC staff submitted a comment to the [National Telecommunications and Information Administration \(NTIA\)](#) on privacy. The comment called for a balanced approach that protects both consumer privacy and innovation, citing the FTC's extensive experience in protecting consumer privacy and fostering innovation. The comment reiterated the FTC's commitment to data security, summarized

the importance of companies' making accurate disclosures about privacy, and called for a balanced approach to choice, where the level of control would depend on consumer preferences, context, and risk. It noted that the Commission should continue to be the primary enforcer of laws related to information flows in the marketplace, whether under the existing or a new privacy and security framework. The comment further noted that both Congress and the Administration are considering federal privacy legislation, and that the Commission strongly supports those efforts.

- ▶ The Commission provided testimony reiterating its commitment to consumer privacy and data security enforcement before both the [Senate Commerce Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security](#) and the [House Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection](#). The Commission also renewed its longstanding bipartisan call for comprehensive data security legislation and urged Congress to consider enacting privacy legislation that would be enforced by the FTC.
- ▶ The FTC testified before the [Senate Banking, Housing and Urban Affairs Committee](#) that enforcement of the FCRA remains a top priority, and outlined the agency's efforts to educate consumers and businesses about the law's requirements. The testimony also outlined the key role the Commission has played in the implementation, enforcement, and interpretation of the FCRA since its enactment in 1970. The testimony noted that in just the last decade the FTC has brought more than 30 actions against consumer reporting agencies, users of consumer reports, and furnishers of information to consumer reporting agencies.

RULES

Congress has authorized the FTC 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. This year, the [FTC announced a regulatory review](#), in which it is seeking public comment to determine whether it should update the Rule in light of new developments in the marketplace.
- ▶ The [COPPA Rule](#) requires websites and apps to get parental consent before collecting personal information from children under 13. The Rule was revised in 2013 to strengthen childrens' 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.

- ▶ The [Telemarketing 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 telemarketing 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.
- ▶ In May, Congress amended the Fair Credit Reporting Act requiring the FTC to issue a Rule requiring nationwide consumer reporting agencies to provide free electronic credit monitoring services for active duty military consumers. In November, the FTC issued a [Notice of Proposed Rulemaking](#) that would require the nationwide consumer reporting agencies to notify active duty military consumers within 24 hours of any “material” additions or modifications to their credit files. In addition to defining key terms, the proposed rule specifies how military consumers may prove their active duty status. The proposed rule also prohibits the consumer reporting agencies from engaging in certain conduct, such as representing that consumers must purchase a product or service in order to obtain the free credit monitoring service.

WORKSHOPS

Beginning in 1996, the FTC has hosted **more than 70** workshops, town halls, and roundtables bringing together stakeholders to discuss emerging issues in consumer privacy and security. In 2018, the FTC hosted the following privacy events:

- ▶ In February, the Commission hosted its third annual [PrivacyCon](#), a conference to examine cutting-edge research and trends in protecting consumer privacy and security. The event brought together leading stakeholders, including researchers, academics, industry representatives, federal policymakers, and consumer advocates. PrivacyCon 2018 explored the privacy and security implications of emerging technologies, such as the Internet of Things, artificial intelligence, and virtual reality. The 2018 event focused on the economics of privacy, including how to quantify the harms that result from companies’ failure to secure consumer information, and how to balance the costs and benefits of privacy-protective technologies and practices.



- ▶ In June, the Commission hosted [Decrypting Cryptocurrency Scams](#), the Commission’s first-ever workshop examining fraudulent practices involving cryptocurrency. The half-day event brought together representatives from consumer groups, law enforcement, research organizations, and the private sector.
- 
- ▶ In November, as part of its public [Hearings on Competition and Consumer Protection in the 21st Century](#), the Commission held a hearing on the intersection of [big data, privacy, and competition](#). The hearing examined the role that data play in competition and innovation. Participants discussed how developments involving data have changed the understanding and use of personal or commercial information; whether stakeholders have policy recommendations on how data can facilitate competition; and whether the presence of personal information or privacy concerns inform or change competition analysis.
 - ▶ In November, the Commission also held a hearing to examine competition and consumer protection issues associated with the use of [algorithms, artificial intelligence, and predictive analytics](#) in business decisions and conduct, as part of its [public hearings initiative](#). The hearing focused on the current and potential uses of these technologies; the ethical and consumer protection issues that are associated with the use of these technologies; how the competitive dynamics of firm and industry conduct are affected by the use of these technologies; and policy, innovation, and market considerations associated with the use of these technologies.
 - ▶ In December, as part of its [public hearings initiative](#), the Commission hosted a [hearing on data security](#), which included discussions related to data breaches and data security threats. The hearing examined incentives to invest in data security, consumer demand for data security, data security assessments, the U.S. framework related to consumer data security, and the FTC’s data security enforcement program.

REPORTS AND SURVEYS

The FTC is a leader in developing policy recommendations related to consumer privacy and data security. The FTC has authored **over 60 reports**, based on independent research as well as workshop submissions and discussions, involving privacy and security. In 2018, the FTC released the following:

- ▶ In February, FTC staff released [Mobile Security Updates: Understanding the Issues](#), a staff report that explores the complexities of mobile operating system patching. Based primarily on patching data collected from eight mobile device manufacturers, the report offers unique insight into security updates practices across the industry. The report made recommendations for streamlining the update process, educating consumers about the importance of updates, and providing timely updates to all mobile devices for a period of time consistent with consumers’ reasonable expectations.
- 
- ▶ FTC staff issued a staff perspective outlining key takeaways from last year’s FTC [workshop on connected cars](#) held jointly with the National Highway Traffic Safety Administration. The staff perspective notes that many different entities throughout the connected car ecosystem will collect data from vehicles that will deliver many beneficial innovations – including faster emergency response, shorter commutes, and more tailored entertainment choices. The staff perspective states that the types of data collected will range from aggregate statistics, to non-sensitive data about a particular car or driver, to sensitive personal information. Given the breadth of this information, consumers may be concerned about unexpected secondary uses of that data. The perspective further indicated that connected and

autonomous cars will have cybersecurity risks that could potentially be exploited by hackers looking to extort money or even do physical harm. To address those concerns, workshop participants discussed best practices, including information sharing, network design, risk assessment and mitigation, and standard setting.

- ▶ FTC staff released a staff perspective outlining key takeaways from a December 2017 [workshop examining informational injuries](#) that consumers may suffer from privacy and security incidents. The staff perspective discussed examples of non-financial harm consumers suffer as a result of such incidents, including medical identity theft, doxing (the deliberate and targeted release of private information about an individual), disclosure of private facts, and erosion of trust. The paper also discusses how the risk of injury must be balanced with the benefits that can come from information collection.



- ▶ FTC staff released [a staff perspective](#) outlining the FTC's plans to develop and distribute reader-friendly educational materials with information about cybersecurity that small businesses need. The effort grew out of the [Small Business & Cybersecurity Roundtables](#) that the FTC hosted in 2017 with small business owners and non-profit organizations, employees, and managers to learn about the challenges they face when dealing with cyber threats and security and ideas for how the government can help them.

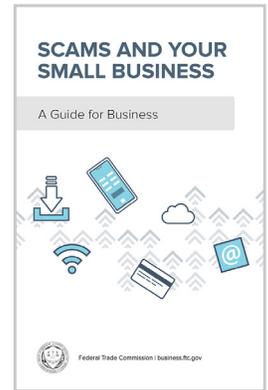


CONSUMER EDUCATION AND BUSINESS GUIDANCE

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**, many of which are published in both English and Spanish, 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 2018 include:

- ▶ The FTC, along with the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and the Small Business Administration (SBA), [launched a national education campaign](#) to help small business owners understand common cyber threats and how they can help protect their businesses. The campaign materials include fact sheets, videos, and quizzes covering a dozen topics, including cybersecurity basics, understanding the NIST Cybersecurity Framework, vendor security, and cyber insurance. The campaign grew out of [a series of roundtable discussions](#) that the FTC held with small business owners last year to discuss cybersecurity challenges they face.
- ▶ The FTC held a series of webinars and conducted social media outreach as part of [Tax Identity Theft Awareness 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's new online consumer education about [Virtual Private Network Apps](#) offers basic information about how the networks work, and what consumers should do and think about before downloading an app.

- ▶ In June, the FTC issued [Scams and Your Small Business: A Guide for Business](#), with to-the-point tips to help small business owners spot the signs of a scam and know what to do if a con artist targets their company. The publication includes tips on phishing, ransomware, social engineering, tech support scams, and call spoofing.
- ▶ As a result of amendments to Fair Credit Reporting Act, in September, free credit freezes and year-long fraud alerts became available for the first time. To help people understand their rights, the FTC published a new consumer [Credit Freeze FAQ](#), a blog for [businesses](#), and three consumer blogs — for [general audience](#), [military consumers](#), and [caregivers](#). In addition, FTC staff revised more than a dozen print publications and online articles in English and Spanish to include the credit freeze and fraud alert changes.
- ▶ The FTC’s [consumer blog](#) alerts readers to potential privacy and data security hazards and offers tips to help them protect their information. In 2018, the most-read consumer blog posts addressed how to [block and report unwanted calls](#) from spoofed numbers, and how to avoid [Social Security Administration imposters](#).
- ▶ The FTC’s [Business Blog](#) addresses recent enforcement actions, reports, and guidance. In 2018, there were 38 data security and privacy posts published on the Business Blog. The most-read posts among them addressed topics including the FTC’s complaint challenging aspects of a [peer-to-peer payment service’s](#) privacy and security practices; a [settlement with a kids’ electronic learning products company](#) for COPPA violations related to data security and storage; and [COPPA’s requirement that businesses delete](#) kids’ personal information under some circumstances.



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 2018 include:

- ▶ The FTC collaborated with the Office of the Privacy Commissioner of Canada (OPC) in the agency’s first-ever enforcement action involving connected toys against [VTech](#), a Hong Kong-based electronics toy manufacturer. In a coordinated release, the FTC announced its complaint and settlement, discussed above, and the OPC issued its own Report of Findings, which found the connected toy maker had failed to adopt adequate security measures to protect children’s sensitive personal information. To facilitate cooperation with OPC, the FTC relied on key provisions of the U.S. SAFE WEB Act.

- ▶ The FTC hosted the 49th [Asia Pacific Privacy Authorities forum](#) in San Francisco. Representatives of 18 agencies from 13 countries discussed members' privacy investigations and enforcement actions, as well as opportunities and challenges relating to artificial intelligence, data breach notifications, and cross-border enforcement cooperation.
- ▶ As part of its work on the management committee of the Global Privacy Enforcement Network (GPEN), the FTC helped to organize a series of teleconference calls and the second GPEN enforcement workshop. During 2018, GPEN grew to include 69 privacy authorities from 50 countries, with over 350 staff from participating agencies registered on an internal GPEN discussion forum.

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 second Annual Review of the EU-U.S. Privacy Shield Framework, the FTC played a leading role in policy deliberations and projects on privacy and data security internationally. For example, the FTC participated in meetings and activities of the APEC Electronic Commerce Steering Group, the International Working Group on Data Protection in Telecommunications, and the Organisation for Economic Co-operation and Development (OECD), providing input on issues ranging from children's privacy, to health-related privacy, to the interoperability of privacy regimes.

The FTC also engaged directly with numerous counterparts on privacy and data security issues. The Commission hosted delegations and engaged in bilateral discussions with officials from Brazil, Costa Rica, France, Japan, South Korea, and the United Kingdom; members of the European Parliament; and European data protection authorities.

Additionally the FTC conducted technical cooperation missions on privacy and cross-border data transfer issues in India and Mexico.



Federal Trade Commission
ftc.gov