Federal Trade Commission 2020 Privacy and Data Security Update

Federal Trade Commission
2020

Federal Trade Commission
2020 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 was established more than a century ago, and throughout its history has endeavored to adapt its enforcement approach to changing market demands, including by developing a privacy and data security program. 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 Gramm-Leach-Bliley Act, the Truth in Lending Act, the Controlling the Assault of Non-Solicited Pornography and Marketing (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. The Commission has used its authority 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?

In the absence of comprehensive general privacy legislation, the FTC has relied on enforcement actions under the general FTC Act and narrower specific statutes as its principal tool to stop law violations and require companies to take steps to remediate the unlawful behavior. This has included 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 transparency and choice mechanisms to consumers. If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations. In some instances, the FTC can also seek 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 CAN-SPAM Act.

Using its existing authority, the Commission has brought hundreds of privacy and data security cases to date. To better equip the Commission to meet its statutory mission to protect consumers, the FTC has also called on members of Congress to enact comprehensive privacy and data security legislation, enforceable by the FTC. The requested legislation would expand the agency's civil penalty authority, provide the agency with more efficient rulemaking authority, and extend the agency's commercial sector jurisdiction to non-profits and common carriers as well.

[1] This document covers the time period from January 2020–December 2020. It will be re-issued on an annual basis.

Beyond case-by-case enforcement, the FTC also develops, amends, and enforces various rules related to privacy and data security. The FTC's rulemaking authority includes specific authority, for example, to issue rules implementing COPPA using the Administrative Procedures Act, and more general authority to address prevalent unfair or deceptive trade practices using Section 18 of the FTC Act. The Commission's 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 consistent: to safeguard consumers' personal information; protect them from illegal practices; and to ensure that consumers have the confidence to take advantage of the many benefits of products offered in the marketplace.

The FTC also takes seriously its obligations to refine its approach by evaluating the effectiveness of its current enforcement strategy and remedies. The Commission is continually looking for ways to better protect consumers' privacy and personal information and prevent unfair data practices.

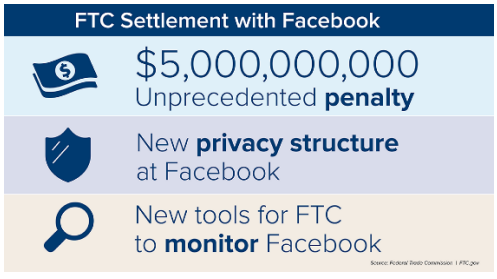
ENFORCEMENT

The FTC, building on decades of experience in consumer privacy enforcement, continued in 2020 to conduct investigations and bring cases addressing practices offline, online, and in the mobile environment, which help protect the greatest number of consumers, as described below. The FTC's cases generally focus on protecting American consumers, but in some cases also protect foreign consumers from unfair or deceptive practices by businesses subject to the FTC's jurisdiction.

General Privacy

The FTC has brought enforcement actions addressing a wide range of privacy issues in a variety of industries, including social media, ad tech, and the mobile app ecosystem. These matters include **more than 130 spam and spyware cases** and **approximately 80 general privacy lawsuits** in the last 20 years, which have affected hundreds of millions of consumers. In 2020, the FTC announced the following privacy cases:

- In April, the United States District Court for the District of Columbia approved the 2019 settlement between Facebook and the Commission and the U.S. Department of Justice. More than 100 million consumers use Facebook every day to share personal information. The complaint alleged that



Facebook violated the Commission's 2012 order against the company by misrepresenting the control users had over their personal information, which tens of millions of users relied upon, and failing to institute and maintain a reasonable program to ensure consumers' privacy. It also alleged that Facebook deceptively failed to disclose that it would use phone numbers provided by users for two-factor authentication for targeted advertisements to those users. The Facebook order imposed a $5 billion penalty, as well as a host of modifications to the Commission's order designed to change Facebook's overall approach to privacy. The $5 billion penalty against Facebook is the largest ever imposed on any company for violating consumers' privacy.

- In November, Zoom, which saw its user base grow from 10 million to 300 million during the COVID-19 pandemic, agreed to settle FTC allegations that, since at least 2016, the company misled users by claiming that it offered "end-to-end, 256-bit encryption" to secure users' communications, when, in fact, it provided a lower level of security. According to the FTC's complaint, Zoom also misled some users who wanted to store recorded meetings on the company's cloud storage by falsely claiming that those meetings were encrypted immediately after the meeting ended. Instead, some recordings allegedly were stored unencrypted for up to 60 days on Zoom's servers before being transferred to its secure cloud storage. Finally, Zoom secretly installed software, called a ZoomOpener web server, as part of a manual update for its Mac desktop application in July 2018. The ZoomOpener web server allowed Zoom to automatically launch and join a user to a meeting by bypassing an Apple Safari browser safeguard that protected users from a common type of malware. Without the ZoomOpener web server, the Safari browser would have provided users with a warning box, prior to launching the Zoom app, which asked users if they wanted to launch the app. The software remained on users' computers even after they deleted the Zoom app, and would automatically reinstall the Zoom app—without any user action—in certain circumstances. The complaint alleges that Zoom's deployment of the ZoomOpener, without adequate notice or user consent, was unfair and deceptive in violation of the FTC Act. Under the proposed settlement, Zoom is prohibited from making misrepresentations about its privacy and security practices. The company must also implement a comprehensive information security program that requires Zoom to implement specific measures aimed at addressing the problems identified in the complaint. The company must obtain biennial assessments of its security program by an independent third party, which the FTC has authority to approve, and notify the Commission if it experiences a data breach.

Data Security and Identity Theft

Since 2002, the FTC has brought **80 cases** against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data. In 2020, the FTC continued to apply its strengthened orders in data security cases in order to provide protection for consumers and accountability for businesses. Each of the cases discussed below resulted in settlements that, among other things, required

the company to implement a comprehensive security program, obtain robust biennial assessments of the program, and submit annual certifications by a senior officer about the company's compliance with the order.

- Tapplock follows a long line of FTC cases related to the Internet of Things and is the first case to allege both data security and physical security vulnerabilities in an Internet-connected device. Tapplock settled FTC allegations that it deceived consumers by falsely claiming that its Internet-connected smart locks were designed to be "unbreakable" and that it took reasonable steps to secure the data it collected from users. According to the FTC's complaint, a vulnerability on Tapplock's API allowed researchers to bypass account authentication and gain full access to all information in Tapplock users' accounts, including usernames, email addresses, profile photos, location history and precise geolocation of the smart lock. Another vulnerability let researchers lock and unlock any nearby Tapplock smart lock. The settlement bans Tapplock from making deceptive statements about security of a device or privacy of personal information. It also requires Tapplock to implement a comprehensive security program, including employee training. Finally, the company must get biennial third-party assessments and must certify compliance annually.

- In its settlement with SkyMed International, Inc., a company that sells air evacuation plans and other travel emergency services, the FTC alleged SkyMed failed to employ reasonable measures to secure the personal information it collected from people who had signed up for its emergency travel membership plan, and, as a result, the company left unsecured a cloud database containing approximately 130,000 membership records. The FTC also alleged that SkyMed misrepresented to consumers that it had investigated the data exposure and concluded that no medical data had been exposed, and that the database had not been improperly accessed when, in fact, SkyMed had not investigated the incident and instead merely deleted the database. The complaint also alleged SkyMed deceived consumers by displaying for nearly five years a "HIPAA Compliance" seal on every page of its website, which gave the impression that its privacy policies had been reviewed and met the security and privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA). In fact, no government agency or other third party had reviewed SkyMed's information practices for compliance with HIPAA. Under the settlement, SkyMed is prohibited from misrepresenting how it secures personal data, the circumstances of and response to a data breach, and whether the company has been endorsed by or participates in any government-sponsored privacy or security program. The company also will be required to send a notice to affected consumers detailing what data was exposed in the security incident. Finally, SkyMed must put in place a comprehensive information security program and obtain biennial assessments of its information security program by a third party, which the FTC has authority to approve. The settlement also requires a senior SkyMed executive to certify annually that the company is complying with the requirements of the settlement.

- In the case of Ascension Data & Analytics, LLC, a mortgage industry data analytics company, Ascension hired a vendor to perform text recognition scanning on mortgage documents. The vendor, OpticsML, stored the contents of the documents in two misconfigured cloud storage locations, without any protections to block unauthorized access. As a result, the sensitive personal information of more than 60,000 consumers was left exposed on the internet for a year. In its complaint, the FTC alleged that Ascension violated the Gramm-Leach-Bliley Act's Safeguards Rule, which requires financial institutions to develop, implement, and maintain a comprehensive information security program. As part of that program, financial institutions must oversee their third-party vendors, by ensuring they are capable of implementing and maintaining appropriate safeguards for customer information, and requiring them to do so by contract. They must also identify reasonably foreseeable risks to customer information and assess the sufficiency of any safeguards in place to control those risks. The FTC alleged that, with respect to its vendors such as OpticsML, Ascension failed to do both. As part of a proposed settlement resolving FTC allegations, Ascension will be required to implement a comprehensive data security program with audits, executive certification, and reporting of future data breaches.

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 **more than 100 cases** against companies for violating the FCRA and has collected **more than $65 million in civil penalties**. These cases have helped insure that consumer reporting agencies follow reasonable procedures to assure the maximum possible accuracy of consumer report information, so consumers can obtain credit, insurance, employment, and housing. The Gramm-Leach-Bliley (GLB) Act requires financial institutions to send customers 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, in order to protect the sensitive personal information consumers provide to them. Since 2005, the FTC has brought about **35 cases** alleging violations of the GLB Act and its implementing regulations, which have affected the data security of hundreds of millions of consumers. The Fair Debt Collection Practices Act (FDCPA) covers third-party debt collectors that collect on consumer debt. The FDCPA addresses abusive, deceptive, and unfair debt collection practices, prohibits certain collection tactics, and imposes certain affirmative statutory obligations on collectors. In 2020, the FTC brought the following credit reporting and financial privacy cases:

- Mortgage Solutions FCS, doing business as Mount Diablo Lending, and its sole owner, Ramon Walker, agreed to pay $120,000 to settle FTC allegations that they violated the FCRA and other laws by revealing personal information about consumers in response to negative reviews posted on the review website Yelp. In a complaint filed by the Department of Justice on behalf of the Commission, the FTC alleged that Mount Diablo Lending and Walker responded to consumers

of medical debt, which is often a source of confusion and uncertainty for consumers because of the complex, opaque system of insurance coverage and cost sharing. The FTC's complaint alleges violations of the FDCPA (including the first federal law enforcement count addressing debt parking), the FCRA, and the FCRA's Furnisher Rule. Under a November 2020 settlement, Midwest Recovery Systems and its owners are prohibited from debt parking and required to delete the debts they previously reported to credit reporting agencies. The settlement includes a monetary judgment of $24.3 million, which is partially suspended based on an inability to pay. Brandon Tumber, one of the individual defendants and a co-owner of the company, will also be required to sell his stake in another debt collection company and provide the proceeds from that sale to the FTC. In addition, the company will be required to surrender all of its remaining assets. This action marks the first federal law enforcement action against unlawful debt parking, and protects consumers dealing with time-sensitive transactions, such as job searches and home loans, from inaccurate or invalid debts appearing on their credit reports without notice.

International Enforcement

For more than two decades, the FTC has used its enforcement powers to ensure strong privacy protections for consumer data subject to international data transfer mechanisms, such as the EU-U.S. Privacy Shield Framework (and its predecessor program, the U.S.-EU Safe Harbor Framework), the Swiss-U.S. Privacy Shield Framework, and the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules System (APEC CBPRs). On July 16, 2020, the European Court of Justice issued a judgment declaring invalid under EU law the European Commission's Privacy Shield Adequacy Decision of July 12, 2016, and in so doing found the EU-U.S. Privacy Shield Framework inadequate under EU law. On September 8, 2020, the Swiss Federal Data Protection and Information Commissioner issued a position statement adopting the European Court's views. The U.S. Department of Commerce announced, after the EU Court's ruling and the Swiss statement, that these developments do not relieve participants of their obligations under either the EU-U.S. Privacy Shield or the Swiss-U.S. Privacy Shield Framework.

Following the European Court's decision, the FTC stated that companies should continue to comply with their ongoing obligations with respect to transfers made under the Privacy Shield Framework. The FTC encouraged companies to continue to follow robust privacy principles, such as those underlying the Privacy Shield Framework, and to review their privacy policies to ensure they describe their privacy practices accurately, including with regard to international data transfers. Although the European Court of Justice invalidated the Privacy Shield Framework under EU law, that decision does not affect the validity under U.S. law of the FTC's decisions and orders, which typically prohibit companies not just from misrepresenting their compliance with or participation in the Privacy Shield Framework, but also in any other privacy or data security programs sponsored by the government or any self-regulatory or standard-setting organization.

Overall, the FTC has brought **66 actions** to enforce companies' promises under these international privacy programs, 39 under the previous "U.S.-EU Safe Harbor" program, 4 under APEC CBPR, and 23 under Privacy Shield. In 2020, the FTC resolved the following matters arising under the Privacy Shield Framework:

- The Commission began the year with a number of Privacy Shield cases involving misrepresentations of participation in and compliance with the EU-U.S. Privacy Shield Framework. In January, following a public comment period, the Commission finalized its Privacy Shield settlements with Click Labs, Inc., DCR Workforce, Inc., EmpiriStat, Global Data Vault, LLC, LotaData, Inc., Incentive Services, Inc., Medable, Inc., TDARX, Inc., Thru, and Trueface.ai.

- In its first Privacy Shield litigation, the Commission sued RagingWire Data Centers, Inc. administratively over allegations that the company misled consumers about its participation in the EU-U.S. Privacy Shield Framework and failed to adhere to the program's requirements before allowing its certification to lapse. In October, the Commission finalized its settlement with NTT Global Data Centers Americas, Inc. (NTT Global Data Centers), formerly known as RagingWire Data Centers. Under the settlement, the company, among other things, is prohibited from misrepresenting its compliance with or participation in the Privacy Shield Framework as well as any other privacy or data security program sponsored by the government or any self-regulatory or standard-setting organization. The company also must continue to apply the Privacy Shield requirements or equivalent protections to personal information it collected while participating in the Framework or return or delete the information. Although the European Court of Justice invalidated the Privacy Shield Framework in July 2020, that decision does not affect the validity of the FTC's decision and order relating to NTT Global Data Centers' misrepresentations about its participation in and compliance with the Framework.

- The FTC charged that Ortho-Clinical Diagnostics, a provider of medical diagnostic devices, misled consumers about its participation in the Privacy Shield Framework. The FTC alleged that the company claimed to participate in the Privacy Shield Framework and comply with the program's requirements, even though the company had allowed its certification to lapse in 2018. The FTC also alleged Ortho violated the Privacy Shield principles by failing to verify annually that statements about its Privacy Shield practices were accurate. In addition, it also allegedly failed to comply with a Privacy Shield requirement to affirm that the company would continue to apply Privacy Shield protections to personal information collected while participating in the program.

- The FTC charged that T&M Protection Resources, a background check services provider, misrepresented its participation in and compliance with the Privacy Shield Framework. The company continued to claim participation in the EU-U.S. Privacy Shield after its certification lapsed. In addition, the company failed to verify annually that statements about its Privacy Shield practices were accurate

and failed to affirm that it would continue to apply Privacy Shield protections to personal information collected while participating in the program.

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 age 13. Since 2000, the FTC has brought **34 COPPA cases** and collected **more than $190 million** in civil penalties. During the past year, the Commission took the following actions:

- The Commission imposed a $4 million civil penalty on children's app developer, HyperBeard, for its COPPA violations, which was partially suspended based on inability to pay. In a complaint filed by the Department of Justice on behalf of the FTC, the Commission alleges that HyperBeard, Inc. violated the COPPA Rule by allowing third-party ad networks to collect personal information in the form of persistent identifiers to track users of the company's child-directed apps, without notifying parents or obtaining verifiable parental consent. The ad networks used the identifiers to target ads to children using HyperBeard's apps. To settle FTC allegations, the company agreed to pay $150,000 and to delete personal information it illegally collected from children under age 13.

- Miniclip, S.A., a Swiss-based company that makes mobile and online digital games, falsely claimed from 2015 through mid-2019 that it was a current member of the Children's Advertising Review Unit's (CARU) COPPA safe harbor program even though CARU terminated Miniclip's membership in 2015. In July 2020, the Commission approved a settlement to resolve allegations that Miniclip violated Section 5 by misrepresenting its status in a COPPA safe harbor program. As part of the settlement, Miniclip is prohibited from misrepresenting its participation or certification in any privacy or security program sponsored by a government or any self-regulatory organization, including the CARU COPPA safe harbor program. Miniclip is also subject to compliance and recordkeeping requirements.

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 **241 million 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, using robocalls to contact consumers to sell goods or services, and calling consumers using spoofed caller ID numbers. Since 2003, the FTC has brought **151 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 510 companies and 404 individuals involved. The 147 cases concluded thus far have resulted in orders totaling more than $1.8 billion in civil penalties, redress,

or disgorgement, and actual collections exceeding $290 million. These actions have halted billions of abusive and fraudulent calls that invade consumers' privacy and cause significant economic harm. During the past year, the Commission initiated actions and settled or obtained judgments as described below:

- Satellite television provider Dish Network agreed to pay $210 million to resolve litigation brought by the Department of Justice on behalf of the FTC, as well as the states of California, Illinois, North Carolina, and Ohio, following remand from the Seventh Circuit Court of Appeals on the issue of the civil penalty amount. Dish Network and its dealers violated consumers' privacy by initiating or causing the initiation of tens of millions of calls to phone numbers on the Do Not Call Registry, using pre-recorded messages, and calling consumers who had previously told Dish or its dealers they did not want to receive calls. The civil penalty award included $126 million penalty for federal violations, which is a record in a DNC case. The remaining penalties were awarded to the states. The settlement came after more than a decade of litigation.

- In the Educare action, the FTC and the Ohio Attorney General reached settlements with defendants that ran a fraudulent credit card rate reduction scheme, including four individuals and six corporate entities. One defendant, Globex Telecom, Inc., is a provider of Voice over Internet Protocol (VoIP) services that transmitted the illegal robocalls for the enterprise. This marks the FTC's first enforcement action taken, and first court order obtained, against a VoIP provider. Globex agreed to pay $1.95 million, which will be used to compensate victims of the scam, and is now required to abide by detailed client screening and monitoring provisions. For example, Globex will not provide VoIP and related services to clients who pay with stored value cards or cryptocurrency, or to clients who do not have a public-facing website or social media presence. In addition, Globex will be required to block any calls made by its clients that appear to come from certain suspicious or spoofed phone numbers, and to terminate their relationship with any telemarketer or other high-risk client that receives three or more USTelcom Traceback Requests (an official industry complaint about unlawful calls) or line carrier complaints in a 60-day period.

- In Alcazar Networks, the FTC's second case against a VoIP provider, the FTC charged that defendants facilitated tens of millions of illegal telemarketing phone calls, including some calls from overseas, and continued to do so even after learning that customers were using the service to initiate calls to numbers on the FTC's Do Not Call (DNC) Registry and calls displaying spoofed caller ID numbers, including displaying "911." The defendants provided VoIP services to an Indian VoIP provider named E. Sampark, who the Department of Justice later criminally prosecuted for sending tens of millions of scam calls from India-based call centers to victims in the United States. Another Alcazar customer, Derek Bartoli, was previously sued by the FTC for making more than 50 million illegal telemarketing calls using Alcazar's services. The order settling the FTC's complaint against Alcazar and its owner permanently bans the defendants from assisting telemarketers or overseas customers with dialing robocalls or calls to

phone numbers on the DNC Registry—regardless of whether those customers purportedly have permission to do so. In addition, the order requires the defendants to block calls that display the caller ID number as "911," related emergency numbers, or unassigned or invalid numbers, and to screen current and prospective customers before providing them with VoIP services. The order imposes a $105,562 monetary judgment against the defendants.

- As part of Operation Income Illusion, a government crackdown on deceptive income schemes undertaken as scammers worked to leverage pandemic fears, the FTC took action against Randon Morris and his companies. A federal court granted the FTC's request for a temporary restraining order against the defendants, who initiated millions of robocalls nationwide to promote sham work-from-home business opportunity programs. The defendants lured consumers into purchasing these programs with false promises that consumers could earn hundreds of dollars a day and claimed an affiliation with Amazon.com where none existed. They also invoked the coronavirus pandemic in robocall messages to prey on consumers who are concerned about working outside of their homes during a national public health crisis. The temporary restraining order stops the defendants' deceptive sales practices, freezes their assets, and appoints a receiver over the companies.

- In Outreach Calling, the FTC and the Attorneys General of New York, Virginia, Minnesota, and New Jersey took on a sprawling fundraising operation that allegedly scammed consumers out of millions of dollars. Defendants served as the primary fundraisers for a number of sham charities that were the subject of numerous law enforcement actions. The sham charities claimed to use consumers' donations to help homeless veterans, retired and disabled law enforcement officers, breast cancer survivors, and others in need. In fact, these organizations spent almost none of the donations on the promised activities. As much as 90 percent of the money raised by the defendants for these sham charities went to the defendants themselves as payment for their fundraising services. What little money the charities did receive was rarely spent on any of their supposedly charitable missions—sometimes less than two percent. The defendants orchestrated the sham charities' fundraising operations by soliciting donations, writing fundraising materials, and providing other key support to the sham charities. Defendants placed calls misrepresenting how donations would be used, and in many instances, the calls violated consumers' do-not-call requests. Under their settlements with the FTC and the states, the defendants are permanently prohibited from participating in any charity fundraising, and from deceiving consumers in any other fundraising effort, including for political action committees (PACs). The defendants are required to clearly inform consumers at the time they ask for money that any donations are not charitable and not eligible for tax deductions. In addition, the defendants are subject to significant monetary judgments and are required to surrender assets. The funds being surrendered by the defendants will be paid to the State of New York, which will contribute the funds on behalf of New York, Virginia, and New Jersey to legitimate charities that perform services that mirror those promised by the sham charities.

- In Grand Bahama Cruise Line, the defendants allegedly made or facilitated millions of illegal calls to consumers nationwide pitching free cruise vacations between Florida and the Bahamas. The defendants' telemarketing operation bought call lists from lead generators that conducted illegal survey robocalls to identify potential customers. In addition to delivering millions of illegal robocalls, the defendants never scrubbed their lists against the agency's Do Not Call Registry and called phone numbers on the Registry. The defendants also illegally called consumers who asked not to be called and used spoofed caller IDs. Settlements with some of the defendants ban them from robocalling, including assisting others in making robocalls. Litigation continues against lead defendant Grand Bahama Cruise Line.

- The FTC's case against 8 Figure Dream Lifestyle, Online Entrepreneur Academy, and their owners shut down a fraudulent money making scheme that used millions of illegal robocalls to find victims. The defendants made false or unsubstantiated claims about how much consumers could earn through their programs, often falsely claiming that a typical consumer with no prior skills could make $5,000 to $10,000 in 10 to 14 days of buying the program. Under the terms of two stipulated final orders, certain defendants are banned from selling money-making methods and others are banned from selling business coaching programs. Nine of the ten defendants are banned from using robocalls for most purposes, including marketing or advertising. In addition, three defendants are prohibited from selling any investment opportunities. The stipulated final orders impose monetary judgments totaling more than $32 million, which are partially suspended based on the defendants' inability to pay. The defendants have surrendered assets totaling more than $1.25 million to the Commission.

- In First Choice Horizon, the FTC halted a fraudulent credit card interest rate reduction scheme that contacted its victims through illegal robocalls. The defendants targeted seniors and deceptively told consumers that, for a fee, the defendants could lower their interest rates to zero for the life of the debt, thereby saving the consumers thousands of dollars on their credit card debt. The settlement order resolving the FTC's allegations bans the defendants from selling debt relief services and from all telemarketing. It also imposes a judgment of $13,881,865 against the defendants, which will be partially suspended based on their inability to pay. The amount each defendant pays will be based on the assets they are required to liquidate.

- In FTC v. Jasjit Gotra, the FTC reached a settlement with lead defendant Jasjit "Jay" Gotra banning him from nearly all outbound telemarketing. Gotra's company, Alliance Security, is a home security installation company that, directly and through its authorized telemarketers, called millions of consumers whose numbers were on the DNC Registry. The settlement order also prohibits Gotra from violating the FCRA, and bars him from misrepresenting his affiliation or association with any other business. It imposes a $9.85 million civil penalty, of which Gotra will pay $88,000, based on his limited financial resources. In 2019, Alliance Security itself also agreed to a complete ban on all telemarketing.

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 vendors of personal health records and related entities that aren't covered by HIPAA to notify individuals, the FTC, and, in some cases, the media when there has been a breach of unsecured individually identifiable health information. In May, the Commission issued a Request for Public Comment as part of the FTC's systematic review of all current Commission regulations and guides. The comment period closed in August, and the FTC is considering next steps.

- The Red Flags Rule, under the FCRA, 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 Card Issuers Rule, also under the FCRA, requires that debit or credit card issuers establish and implement reasonable policies and procedures to assess the validity of an address change request if, within a short period of time after receiving the request, the card issuer receives a request for an additional or replacement card for the same account. Together, the Red Flags Rule and the Card Issuers Rule are known as the Identity Theft Rules. In 2018, the FTC announced a regulatory review of the Identity Theft Rules, in which it sought public comment on, among other things, the economic impact and benefits of the Rules and whether and how the Rules might need to be modified. The Commission received comments during the public comment period in 2019, and is evaluating next steps.

- The COPPA Rule requires websites and apps to get parental consent before collecting personal information from children under 13. In 2019, as part of its ongoing effort to ensure that its Rules are keeping up with emerging technologies and business models, the Commission announced that it was seeking comment on the effectiveness of the 2013 amendments to the COPPA Rule and whether additional changes are needed. The Commission is reviewing the more than 170,000 submissions received during public comment period.

- 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 GLB Privacy Rule sets forth when car dealerships must provide customers 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. In 2019, the FTC issued a Notice of Proposed Rulemaking and received comments on proposed amendments to both the GLB Privacy and Safeguards Rules. In July 2020, the Commission held

a virtual workshop to examine the amendments to the Safeguards Rule, and received public comments. The FTC is evaluating next steps on both Rules.

- 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 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. Following a public comment period as part of its systemic review of all current FTC rules and guides, in 2019 the FTC determined that it would confirm the CAN-SPAM Rule without change.

- The Disposal Rule, under the Fair and Accurate Credit Transactions Act of 2003, requires that companies dispose of credit reports and information derived from them in a safe and secure manner.

- In 2020, the Commission sought public comment on changes to and effectiveness of five FCRA Rules, and proposed amendments to harmonize the following rules with Dodd-Frank: The Address Discrepancy Rule, which outlines the obligations of users of consumer reports when they receive a notice of address discrepancy from a nationwide consumer reporting agency (CRA); the Affiliate Marketing Rule, which gives consumers the right to restrict a person from using certain information obtained from an affiliate to make solicitations to the consumer; the Furnisher Rule, which requires entities that furnish information to CRAs to establish and implement reasonable written policies and procedures regarding the accuracy and integrity of the information relating to consumers provided to a CRA; the Pre-screen Opt-Out Notice Rule, which 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; and the Risk-Based Pricing Rule, which requires those who use information from a consumer report to offer less favorable terms to consumers to provide them with a notice about the use of such data.

REPORTS AND STUDIES

- Section 6(b) of the FTC Act authorizes the Commission to conduct wide-ranging studies separate from the agency’s law enforcement authority. Under Section

6(b), the Commission may issue Orders requiring companies to file Special Reports. In December 2020, the Commission issued 6(b) orders to nine social media and video streaming services requiring them to provide data on how they collect, use, track, estimate, derive, and present personal and demographic information, their advertising and user engagement practices, and how their practices affect children and teens. The orders were sent to Amazon.com, Inc.; ByteDance Ltd., which operates the short video service TikTok; Discord Inc.; Facebook, Inc.; Reddit, Inc.; Snap Inc.; Twitter, Inc.; WhatsApp Inc.; and YouTube LLC. These recipients will be required to file responses to the 6(b) orders. The information that the Commission obtains from these responses will help inform the Commission's mission of protecting consumers and competition in the marketplace.

- The Commission also filed the following three reports to Congress in 2020:
  - In its report, Fair Credit Reporting Act: Efforts to Promote Consumer Report Accuracy and Disputes, Report to Congress, the Commission updated lawmakers on the agency's efforts to educate consumers about their rights to dispute and correct errors in their credit reports.
  - In its report, Resources Used and Needed for Protecting Consumer Privacy and Security, the Commission provided a comprehensive internal assessment measuring the agency's current efforts related to data privacy and security while separately identifying all resource-based needs of the FTC to improve in these areas.
  - In its report, FTC's Use of its Authorities to Protect Consumer Privacy and Security, the Commission reported on the ways it utilizes its current authorities, including Section 5 unfairness authority, to deter unfair and deceptive conduct in consumer privacy and data security matters.

WORKSHOPS

Beginning in 1996, the FTC has hosted 77 workshops, town halls, and roundtables bringing together stakeholders to discuss emerging issues in consumer privacy and security. In 2020, the FTC hosted the following privacy events:

- Information Security and Financial Institutions: FTC Workshop to Examine Safeguards Rule. In July 2020, the FTC hosted a virtual workshop regarding proposed amendments to the GLB Safeguards Rule, with more than 700 viewers in attendance. Panelists, many of whom are information security professionals at financial institutions covered by the Safeguards Rule, provided empirical data on

the proposed amendments to the GLB Safeguards Rule as part of the federal rulemaking. The archived video and transcripts are available on the event page.

- PrivacyCon 2020. Also in July 2020, the FTC held the fifth PrivacyCon as a virtual workshop, with almost 2,000 unique viewers in attendance. The sessions focused on research related to health apps, artificial intelligence, Internet of Things devices, the privacy and security of specific technologies such as digital cameras and virtual assistants, international privacy (including the GDPR), and a closing session that touched on miscellaneous privacy and security issues, including usability, security scanner performance, and advertising tracking. The archived video and transcripts are posted on the event page. PrivacyCon 2021 is scheduled for July 27, 2021, and the Commission has issued a call for research presentations.

- Data to Go: An FTC Workshop on Data Portability. In September 2020, the FTC held a virtual workshop to examine the potential benefits and challenges to consumers and competition raised by data portability, with more than 880 unique viewers in attendance. Data portability refers to the ability of consumers to move data—such as, emails, contacts, calendars, financial information, health information, favorites, friends or content posted on social media—from one service to another or to themselves. Panelists discussed the status of data portability initiatives in the U.S. and across the world, and also provided analysis on what it takes to realize the benefits data portability promises, and how to make it work. The archived video and transcripts are posted on the event page.

CONSUMER EDUCATION AND BUSINESS GUIDANCE

The Commission has distributed millions of copies of educational materials, many of which are published in both English and Spanish, to help consumers and businesses 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 education and guidance materials developed in 2020 include:

- **Cybersecurity for Small Business Campaign.** The FTC continues to promote the Cybersecurity for Small Business Campaign at ftc.gov/Cybersecurity and, in Spanish,

at ftc.gov/ciberseguridad. In 2020, the agency collaborated with the Cybersecurity and Infrastructure Security Agency (CISA) in the development of its Cyber Essentials Toolkit. In recognition of Cybersecurity Awareness Month, the FTC presented a webinar about connected devices to the National Cybersecurity Alliance (NCSA) and introduced the revised business guidance *Careful Connections: Keeping the Internet of Things Secure*. It also joined hosts NCSA and the Identity Theft Resource Center, dozens of local and national government agencies, and cyber education associations in a Twitter chat to raise awareness about cybersecurity. Other outreach about cybersecurity included a virtual presentation at the New England Library Association's conference and a webinar with women small business owners at a tri-state Small Business Administration (SBA) Women's Business Development Center.

- **Tax Identity Theft Awareness Week.** As part of its 2020 Tax Identity Theft Awareness Week, the FTC hosted outreach events including webinars, telephone town hall meetings, and a Twitter chat to alert consumers, tax professionals, veterans, and small businesses about the ways they can minimize their risk of tax identity theft, and recover if it happens. Working with federal partners throughout the week, including the Department of Veterans Affairs, U.S. Postal Inspection Service, and Internal Revenue Service (IRS), and with organizations like AARP and the Identity Theft Resource Center, the FTC reached more than 13,200 people. These events allowed the FTC and its partners to share information about tax identity theft and imposter scams aimed at getting people's money and their personal information. FTC staff also presented information about tax identity theft to tax professionals and lawyers as part of an IRS working group, and delivered a Tax Security Awareness webinar with the IRS and local Better Business Bureau.

- **Green Lights & Red Flags: FTC Rules of the Road for Business Seminar.** In October 2020, the FTC hosted Green Lights & Red Flags: FTC Rules of the Road for Business, a workshop focused on truth-in-advertising law, data security, social media marketing, and business-to-business fraud. More than 440 business owners and advertising, marketing, and legal professionals registered for the event. Originally planned as a live workshop in Cleveland, the 2020 workshop became the first-ever online session of the popular FTC business seminar series. Co-sponsors included the Ohio Office of the Attorney General, BBB Serving Greater Cleveland, and the Cuyahoga County Department of Consumer Affairs.

- **Identity Theft Program.** When new forms of identity theft and information misuse emerged during the COVID-19 pandemic, the FTC responded with

consumer education and changes to IdentityTheft.gov. For example, in May, the Agency told people they could get free, weekly credit reports and how to order them. The Agency continues to help consumers handle the financial impact of COVID-19.

The FTC changed the wording on IdentityTheft.gov to help people report someone's misuse of their information to claim an Economic Impact Payment and published a blog that explained what to do in case of theft. The FTC later added a button to the IdentityTheft.gov landing page to make it faster for people to report unemployment benefits identity theft, and published a blog with advice about what to do if someone got a notice from their state unemployment benefits office or employer about their supposed application for benefits.

Early in 2020, staff distributed identity theft education material through local libraries, and discussed how to respond to the theft during community meetings with a League of Women Voters and congressional staff. Staff shared identity theft information and FTC resources via webinar with professionals who assist identity theft victims, including legal service providers, volunteers for the Senior Medicare Patrol, and staff in a crime victims' resource center. The FTC continued to collaborate with law enforcement agencies by, for example, co-presenting an identity theft training for community non-profits with an attorney general and US Attorney's office, and teaching a state attorney general's office about FTC identity theft resources.

- **Consumer Blog.** The FTC's Consumer Blog alerts readers to potential privacy and data security hazards and offers tips to help them protect their information. In 2020, the most-read consumer blog posts addressed how to avoid Social Security Administration imposters and what to if scammers ask for money or personal information in exchange for an Economic Impact Payment. Other popular posts explained how to avoid Bitcoin blackmail, dodge text scams posing as package delivery messages, and preserve your privacy and data security during the COVID-19 pandemic. Numerous blogs related to COVID-19 explained how to stay safe while working from home and while videoconferencing; how to keep children safe during remote learning; and what to do if a thief got unemployment benefits in your name.

- **Business Blog.** The FTC's Business Blog addresses recent enforcement actions, reports, and guidance. In 2020, there were 55 data security and privacy posts published on the Business Blog. Highlights include two blogs by the Director of the FTC's Bureau of Consumer Protection: one announcing new and improved data security orders, the other considering the consumer protection implications of artificial intelligence. In 2020, there was also a post analyzing the FTC's proposed settlement with Zoom, which will require the company to honor its security promises and implement a comprehensive program designed to protect

consumers' information. Another post covered a settlement with a company whose smart locks had security vulnerabilities.

The FTC published several blogs to help businesses protect data and privacy during the pandemic, including COPPA guidance for edtech companies and schools, videoconferencing tips for business, advice for companies transferring data to the cloud, and a review of seven common scams targeting businesses.

- **Mobile Device Privacy & Security**. In 2020, the FTC published blogs to help consumers protect their personal information while using mobile devices. A February blog warned that people had reported imposters—posing as a bank or friend in need—using mobile payment apps to steal money. The FTC shared a blog post with tips to help parents protect children's privacy when they use apps—this in response to a settlement with HyperBeard, an app developer that violated the law when it collected personal information from children under age 13.

INTERNATIONAL ENGAGEMENT

Part of the FTC's privacy and data security work is engaging with international partners. The agency works with foreign privacy authorities, international organizations, and global privacy authority networks to develop mutual enforcement cooperation on privacy and data security investigations. The FTC also plays a role in advocating for 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. In 2020, Congress renewed the U.S. SAFE WEB Act for another seven years.

A significant part of the FTC's cooperation efforts in 2020 focused on the response to the COVID-19 pandemic. For example, 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 a virtual roundtable on enforcement and the COVID-19 pandemic for enforcement authorities. GPEN includes 69 privacy authorities from 50 countries, with about 400 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, the FTC played an important role in policy deliberations and projects on privacy and data security internationally, including the global response to the COVID-19 pandemic. For example, the FTC participated in meetings and activities of the Global Privacy Assembly, the APEC Electronic Commerce Steering Group, the Asia-Pacific Privacy Authorities Forum, and the Organisation for Economic Co-operation and Development, providing input on issues ranging from the COVID-19 pandemic to children's privacy and 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 Chile, South Korea, Turkey, and members of the European Parliament. Additionally, the FTC conducted technical cooperation exchanges on privacy and cross-border data transfer issues with Bangladesh, Bermuda, India, and Singapore.

Federal Trade Commission
ftc.gov