The Federal Trade Commission 2023 Privacy and Data Security Update

Federal Trade Commission
2023

The Federal Trade Commission
2023 Privacy and Data Security Update[1]

Preface

by Samuel Levine
Director, Bureau of Consumer Protection

The past three years have been a tremendously busy period for the Commission, and I am particularly proud of our accomplishments in the areas of privacy and data security. We have worked vigorously to ensure that the law has equal force across the digital ecosystem, rising to the challenges presented by new technologies and seeking meaningful remedies that establish critical standards for protecting consumers' information, rather than placing the burden on consumers to protect themselves. This is an area that demands an all-hands-on-deck response, and as the examples in the report show, the Commission is using every tool it has to safeguard consumers' rights. To highlight a few of the agency's achievements:

- **Artificial Intelligence:** The Commission has been leading efforts to ensure that AI and similar technologies are not deployed in harmful ways. In addition to obtaining orders against Rite Aid, Ring, and Amazon to ensure that companies are disincentivized from using data that was wrongfully collected or trained to develop AI, we have initiated a market study of social media and video streaming platforms on the use of AI, announced a public contest to develop new approaches to protect consumers from AI-enabled voice cloning harms, proposed rules to crack down on AI-fueled impersonator and fake review fraud, and issued numerous business guidance alerts.

- **Children and Teens:** The Commission proposed strengthening the Children's Online Privacy Protection Act to make digital services safer and more secure for children, and to put the onus on providers rather than parents to keep kids' data secure. The Commission has also been active in the enforcement arena, obtaining a record-breaking civil penalty settlement with Epic Games, and implementing substantive protections for teens as well, by mandating that settings default to protect their privacy. Our work in the educational technology space—including our case against Edmodo and policy statement on education technology—sent a strong message that businesses cannot outsource compliance when it comes to children's privacy.

[1] This Update covers the time period from January 2021 to December 2023.

- **Sensitive Data:** As the privacy threats from data collection continue to grow, protecting the privacy and security of consumers' sensitive data has continued to be a top Commission priority. The Commission's groundbreaking actions to safeguard health, biometric, and geolocation data—including BetterHelp, GoodRx Holdings, Premom, Flo Heath, RiteAid, and Kochava, along with the InMarket, X-Mode, and Avast cases that were filed after the time period covered by this update—demonstrate that our agency will not tolerate failures to protect consumers' sensitive information at any stage in the data lifecycle.

- **Market-wide Protections:** The Commission initiated rulemaking initiatives to establish sensible and reasonable baselines that protect consumers and put honest businesses on a level playing field. These included amendments to require financial institutions to notify the FTC of large data breaches, notices of proposed rulemaking to clarify the application of the Health Breach Notification Rule to health apps and strengthen the Children's Online Privacy Protection Act Rule, and an advanced notice of proposed rulemaking to explore rules that would crack down on harmful commercial surveillance and lax data security.

While the work of the FTC's attorneys, economists, investigators, technologists, and other specialists has made enormous strides in protecting the privacy and security of consumers' information, there is much more that needs to be done. The explosive growth in data collection and the rapid pace of technological developments that allow information to be exploited in new ways demands action. The Commission has consistently called on Congress to restore its ability under Section 13(b) of the FTC Act to return money to consumers in federal court, and to pass comprehensive privacy legislation. As the data abuses described in this report makes clear, that ask is more urgent than ever.

INTRODUCTION

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 address emerging threats and changing market demands. Over the past several decades, the FTC has demonstrated this ability to adapt in response to the growth of the information economy and increasing collection of data about American consumers through the development of a robust privacy and data security program.

The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act (Section 5), 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 (COPPA), 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. As new technologies and business models have emerged, the Commission has used its authority flexibly to address a wide array of practices affecting consumers' privacy and the security of their information.

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

In the absence of comprehensive federal privacy or data security legislation, the FTC has relied on enforcement actions under the FTC Act and narrower specific statutes to stop law violations and require companies to take steps to remediate unlawful behavior. FTC orders have included implementation of comprehensive privacy and security programs, biennial assessments by independent experts, monetary redress to consumers, deletion of illegally-obtained consumer information and derived data products, and notice to consumers of the alleged law violations. If a company violates an FTC order, the FTC can seek civil monetary penalties for the violations, as it did in the Facebook and Twitter cases discussed below. The FTC can also seek civil monetary penalties for violations of certain privacy statutes and rules, including COPPA, 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 better equip the Commission to meet its statutory mission to protect consumers, the FTC has also called on Congress to enact comprehensive privacy and data security legislation, enforceable by the FTC. The requested legislation would set strong baseline protections for all Americans and provide the FTC with additional tools to protect consumers' privacy.

Beyond case-by-case enforcement, the FTC also develops, amends, and enforces various rules related to privacy and data security, and works to educate both

businesses and consumers about privacy and data security issues. The FTC's rulemaking authority includes specific authority, for example, to issue rules implementing COPPA using the Administrative Procedure Act, and more general authority to address prevalent unfair or deceptive trade practices using Section 18 of the FTC Act. The Commission's tools also include conducting studies and issuing reports, hosting public workshops, developing educational materials for consumers and businesses, testifying before Congress, commenting on legislative and regulatory proposals that affect consumer privacy, and working with international partners on global privacy and accountability issues.

In all its privacy and data security work, the FTC's goals have remained consistent: to provide consumers with substantive privacy protections, safeguard their personal information, and stop abusive and unlawful data practices.

ENFORCEMENT

The FTC, building on decades of experience in consumer privacy and data security enforcement, is taking bold steps to deliver strong privacy protections. The FTC has brought enforcement actions addressing a wide range of privacy issues across multiple industries, including social media, ad tech, and the mobile app ecosystem. These matters include **97 privacy cases** and **169 Telemarketing Sales Rule and CAN-SPAM cases** since 1999, which have affected hundreds of millions of consumers.

In its recent enforcement work, the Commission has specifically focused on issues related to artificial intelligence, health data, geolocation tracking, children and teens' data, data security, credit reporting and financial privacy, and spam calls and emails.

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.

Artificial Intelligence

The Commission has been on the front lines of consumer protection issues involving artificial intelligence (AI), algorithms, and automated tools. In a number of enforcement actions, the FTC has alleged that companies violated the FTC Act or other laws in connection with their collection, retention, or use of consumers' personal information to develop or deploy machine learning or similar algorithms. The FTC has also sought to protect consumers by ensuring that unlawfully obtained or retained data cannot be used to develop algorithms or for machine learning. Recent enforcement actions reflect the Commission's position that there is no AI exception to the law.

- In Rite Aid Corp., the FTC charged that the company acted unfairly in violation of the FTC Act by failing to take reasonable steps to ensure that the AI facial recognition technology it deployed in its retail stores did not erroneously flag

consumers as shoplifters or wrongdoers. While the FTC has previously brought cases relating to misrepresentations about the use of facial recognition technology, this case is the first in which the FTC alleged that the technology was used unfairly. The FTC's complaint alleged that Rite Aid acted unreasonably by failing to consider and address heightened risks of misidentification to women and people of color, failing to assess the accuracy of the technology before deploying it, using low-quality images, failing to train or oversee employees that operated the technology, and failing to monitor the accuracy of the technology and the rate of false positive matches it generated. The settlement that the FTC obtained, which is pending court approval, would ban Rite Aid from using facial recognition technology for security or surveillance purposes for five years. It would also subject any future use of automated biometric security or surveillance systems, including facial recognition technology, to a rigorous monitoring program that would require the company to take steps before and during deployment of the technology to control risks posed to consumers. It would also require that the company cease using such technology if it cannot control such risks.

- A federal court entered an order against Ring, resolving FTC allegations that the maker of connected home security cameras had illegally surveilled customers in private spaces of their homes and had failed to take reasonable steps to prevent hackers from gaining access to customer accounts, live streams of videos, and stored videos. The order requires Ring to delete data products such as data, models, and algorithms derived from videos it unlawfully reviewed.[2] The order also requires Ring to implement a privacy and security program with novel safeguards on human review of videos as well as other stringent security controls, such as multi-factor authentication for both employee and customer accounts. Ring must pay $5.8 million for consumer redress and notify consumers about the FTC action.

- In the Amazon/Alexa matter, the FTC alleged that Amazon violated COPPA and the FTC Act by indefinitely retaining children's voice recordings, which it used to improve its speech recognition algorithm. The FTC also alleged that Amazon failed to honor users', including parents', requests to delete voice and geolocation data, which remained available to Amazon for its own use in improving the Alexa algorithm. Under the FTC's settlement with Amazon, the company is required to delete inactive accounts and certain voice recordings and geolocation information from children, and will be prohibited from using such data to train its algorithms.

- Following announcement of the Amazon/Alexa and Ring matters, Commission staff published guidance on AI and privacy lessons drawn from those

[2] In several actions, including Everalbum, Ring, Amazon/Alexa, CRI Genetics, and Kurbo/Weight Watchers, the FTC has obtained orders that require the deletion of any algorithms or other work product derived from improperly collected information.

enforcement actions. The guidance, Hey, Alexa! What are you doing with my data?, advises companies (among other things) that privacy is an integral component to AI development and use; consumers—not companies—control their data; and that it's important to place special safeguards on human review and employee access to sensitive data.

- In Everalbum, Inc., the FTC alleged that the operator of a mobile app allowing users to upload, store, and organize photos and videos misrepresented the extent of its use of facial recognition technology. Though the company represented that the technology would not be used to process consumers' images unless the consumers opted-in to such processing, for most users the app's facial recognition technology was used by default and could not be turned off. The FTC also alleged the company trained its facial recognition algorithms on user photos. The FTC obtained an order requiring Everalbum to delete its work product, including any models or algorithms, derived from unlawfully obtained or possessed data.

- The Commission recently issued a new omnibus resolution authorizing use of compulsory process for product and services that (1) use or claim to be produced using AI or that (2) claim to detect AI-generated content. The resolution will streamline FTC staff's ability to obtain Commission approval for the issuance of civil investigative demands in investigations involving AI.

Health Privacy and Security

Protecting the privacy and security of consumers' sensitive health information has long been a top Commission priority. Since January 2021, the Commission has brought numerous enforcement actions focused on these issues. Recent health-related orders have imposed strong injunctive relief, requiring businesses to: stop sharing health information with third parties for advertising purposes, obtain affirmative express consent for other disclosures of health data, instruct third parties to delete improperly disclosed data, provide notice to consumers about illegal third-party disclosures, and establish privacy or data security programs without independent assessments. In addition, recent health-related orders have included monetary relief: civil penalties under the Health Breach Notification Rule or redress for consumers.

- The FTC gave final approval to an order banning BetterHelp, an online counseling service, from sharing sensitive health data for advertising with Facebook and other third parties and requiring it to pay $7.8 million to provide partial refunds to consumers. The complaint against BetterHelp makes clear that any information that identifies a consumer as seeking or receiving mental health treatment is health information. The order also requires BetterHelp to institute a comprehensive privacy program, notify consumers that it improperly disclosed their health information to third parties, and instruct third parties to delete the health information disclosed to them by BetterHelp without consumers' affirmative express consent.

- In GoodRx Holdings, Inc., the FTC announced its first enforcement action under its Health Breach Notification Rule. The FTC's complaint alleges that GoodRx, a popular telehealth and prescription discount platform used by tens of millions of American consumers, was disclosing its users' personal health information to advertising platforms like Facebook and Google and, in some cases, using that information to target consumers with health- and medication-specific ads, violating its privacy promises. The FTC's complaint also alleged that the company's data sharing practices were deceptive and unfair, including its alleged unfair failure to maintain sufficient policies or procedures to protect its users' personal health information. Under the stipulated order, GoodRx was required to pay a $1.5 million civil penalty for its alleged failure to comply with the Health Breach Notification Rule. The order also secured strong injunctive relief similar to that obtained in the BetterHelp matter.

- The FTC finalized its settlement with Easy Healthcare Corporation, the publisher of a period and ovulation tracker mobile app called Premom. The FTC complaint alleged that Easy Healthcare shared Premom users' sensitive health information with third parties, such as Google, in the form of "app events," which is app data transferred to third parties for various reasons, and that Easy Healthcare shared Premom users' sensitive, identifiable data with foreign mobile analytics companies. The FTC alleged that Easy Healthcare engaged in unfair and deceptive practices and violated the Health Breach Notification Rule. The stipulated order includes order provisions similar to GoodRx and requires Easy Healthcare to pay a $100,000 civil penalty.

- The FTC entered into a settlement with Flo Health, the developer of a period and fertility-tracking app used by more than 100 million consumers. In an administrative complaint, the FTC alleged that the company disclosed users' sensitive health information, including information about users' pregnancies, with third-party analytics providers, including Facebook and Google, in the form of app events. According to the complaint, Flo had deceptively promised users to keep their health information private, in violation of Section 5. The complaint also alleged that Flo violated the EU-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield frameworks then in place, which required notice, choice, and protection of personal data sent to third parties. Among other things, the FTC's order required Flo to notify users of its violative practices, instruct third parties to delete the data, and obtain an independent compliance review.

- The FTC finalized an administrative complaint and consent order against 1Health.io, doing business as Vitagene, a maker and seller of direct-to-consumer DNA test kits. The FTC's complaint alleges that Vitagene deceived consumers by misrepresenting that it (a) exceeded industry-standard security practices, (b) stored DNA test results without names or other common identifying information, (c) would delete all consumer information upon request, and (d) destroyed consumers' physical DNA saliva samples shortly after analyzing them. The complaint also alleges that Vitagene unfairly adopted material retroactive privacy

policy changes regarding the sharing of consumers' sensitive personal information with third parties. Among other things, the order requires Vitagene to implement and maintain a comprehensive information security program, to obtain initial and biennial third-party assessments of the program, to pay $75,000 for consumer redress, and to instruct laboratories that collected DNA samples for Vitagene to destroy samples.

- In July 2023, following announcement of the Flo Health, GoodRx, BetterHelp, Premom, and Vitagene matters, Commission staff published guidance on "Protecting the privacy of health information: A baker's dozen takeaways from FTC cases," which highlighted thirteen lessons for businesses from these enforcement actions. The guidance offered five lessons on the "basics": understanding what constitutes health information; the obligation to protect the privacy of that information; the privacy risks associated with tracking technologies that use identifying health information; improper disclosure or receipt of health information; and ensuring that technical and compliance staff communicate effectively. The guidance cautioned businesses to avoid making deceptive HIPAA-related claims and to avoid deceptive HIPAA seals and certifications. It also advised businesses on consent and avoiding deceptive euphemisms and omissions. It concluded by emphasizing that health privacy is a top priority for the Commission.

- The FTC and the State of California jointly settled claims against CRI Genetics, LLC, a genetic testing company that provides DNA-based ancestry and other DNA-based health reports to consumers. The FTC and California alleged that CRI made deceptive claims on its websites and social media that its DNA-based ancestry reports were more accurate and detailed than the other major DNA-ancestry testing companies such as AncestryDNA and 23andMe. The complaint also alleged that CRI used manipulative techniques or "dark patterns" to force consumers to click through various pop-up pages for additional products and services with time-urgency and limited-supply claims and misrepresentations in the ordering process, making it impossible for consumers to review and delete their selections before being charged for payment. The company also posted fake DNA test ratings on supposedly unbiased and independent educational websites that they owned and posted fake consumer reviews on their websites. Like the Vitagene settlement (which also involved genetic data), this settlement follows up on the Commission's recent Policy Statement on Biometric Information and Section 5 of the FTC Act . Among other things, the order requires the company to delete DNA and personal information and pay California $700,000 in civil penalties.

Geolocation Tracking

Precise location data is highly sensitive because it can reveal detailed information about an individual, such as their visits to cancer treatment or reproductive clinics, places of worship, or domestic violence shelters. Over the past few years, the FTC has focused

though the following actions on preventing harms to consumers that result from exposure of this sensitive information:

- The FTC filed an enforcement action in Idaho federal court against Kochava Inc. Kochava is a data aggregator that compiles and sells consumers' precise geolocation data gathered from consumers' cell phones. The FTC alleges that Kochava sells this data in a format that makes it easy to track consumers to sensitive locations, such as medical facilities, places of worship, and homeless and domestic violence shelters. The FTC also alleges that Kochava did not have any technical controls to protect consumers' privacy. In denying Kochava's motion to dismiss the FTC's complaint, the Court held that the FTC stated a legally and factually plausible claim that "Kochava's practice of selling vast amounts of data about mobile device users *may* violate Section 5(a) by depriving consumers of their privacy and exposing them to significant risks of secondary harms."[3] This matter remains in active litigation.

- The FTC finalized an administrative settlement with Support King, LLC, formerly doing business as SpyFone.com, and its CEO, Scott Zuckerman, which licensed, marketed, and sold stalkerware apps that allowed purchasers to surreptitiously monitor photos, text messages, web histories, GPS locations, and other personal information of the phone on which the app was installed without the device owner's knowledge. Support King and Scott Zuckerman settled charges alleging that they: unfairly sold stalkerware apps without taking reasonable steps to ensure that the purchasers would use the apps only for legitimate and lawful purposes; misrepresented that they would take all reasonable precautions to safeguard customer information, including by encrypting consumers' personal information stored in their database; and misrepresented that they partnered with leading data security firms to investigate a data breach and coordinated with law enforcement authorities. Among other things, the consent order bans Support King and Scott Zuckerman from offering, promoting, selling, or advertising any surveillance app, service, or business.

- Commission staff published business guidance titled Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data that articulated the potential harms to consumers from exposure of sensitive data and emphasized the Commission's commitment to vigorous law enforcement to protect sensitive data.

Children's Privacy

The Commission also vigorously protects children's personal information, both through enforcement of Section 5 of the FTC Act and the Commission's COPPA Rule, which implements the Children's Online Privacy Protection Act of 1998 (COPPA). The COPPA Rule generally requires websites and apps to obtain verifiable parental consent before

[3] F.T.C. v. Kochava, Inc., Case No. 2:22-CV-00377-BLW, 2024 WL 449363, at *6 (D. Idaho Feb. 3, 2024).

collecting personal information from children under age 13 and imposes other substantive protections for children's personal information. Since 2000, the FTC has brought **42 COPPA cases** and collected **more than $532 million** in civil penalties. Since January 2021, the Commission has taken the following actions to protect the privacy of children's personal information:

- In May 2023, the FTC announced that it was proposing changes to the FTC's 2020 privacy order with Facebook (now Meta) because it had reason to believe the company had failed to fully comply with the COPPA Rule as well as prior FTC orders (both a 2020 and a 2012 Commission order). The FTC alleged that, in certain circumstances, Facebook misled parents about their ability to control with whom their children communicated through its Messenger Kids app, and misrepresented the access it provided some app developers to private user data. The FTC also alleged that Facebook's privacy program, which is mandated by the 2020 order, contained several gaps and weaknesses that posed substantial risks to the public. As part of the proposed changes, Facebook would be prohibited from profiting from data it collects from users under the age of 18. If issued, the proposed modified order would also subject Facebook to other expanded limitations, such as in its use of facial recognition technology. The Commission issued an Order to Show Cause to Facebook (now Meta) why these proposed modifications should not be adopted. This matter remains in active litigation.

- Epic Games, Inc., creator of the popular video game Fortnite, settled in federal court in North Carolina to resolve FTC/DOJ allegations that Epic had violated the COPPA Rule by (a) collecting personal information from children through Fortnite without first notifying their parents or getting their parents' verifiable consent, and (b) failing to allow parents to review and delete the personal information Epic had collected from their children. The complaint also alleged that Epic's matching of children and teens with strangers in Fortnite with on-by-default voice and text chat features was unfair under Section 5 because it subjected those children and teens to bullying, threats, and harassment, and exposed them to dangerous and psychologically traumatizing issues like suicide and self-harm. The order requires Epic to delete personal information that it had unlawfully collected from children, comply with the COPPA Rule going forward, adopt strong privacy default settings for children and teens, implement a privacy program subject to third-party assessments, and pay a record-setting civil penalty of $275 million.

- Amazon, the maker of the Alexa-powered Echo smart speaker, stipulated to a federal court order to resolve FTC/DOJ allegations that it had violated Section 5 and the COPPA Rule by retaining children's voice recordings indefinitely and failing to delete voice recordings and geolocation information upon request, as promised. The complaint also alleged that Amazon engaged in unfair privacy practices by keeping information forever for its own purposes, undermining Alexa users' deletion requests, and subjecting retained data to the risk of unnecessary access. The order requires Amazon to delete inactive child accounts and certain

voice and geolocation information. The order prohibits Amazon from using such information to train its algorithms. The order also requires Amazon to create a privacy program, notify users of the FTC-DOJ action and retention/deletion controls, and pay a $25 million civil penalty.

- Educational technology company Edmodo entered into a federal court order to resolve FTC allegations that it violated COPPA by failing to obtain verifiable parental consent before collecting children's personal information, and that it unlawfully outsourced its COPPA compliance responsibilities to schools. Edmodo was charged with illegally collecting and retaining children's personal information, and unfairly requiring schools and teachers to comply with the COPPA Rule on its behalf. The August 2023 federal court order against Edmodo imposed a civil penalty as well as injunctive relief, including banning Edmodo from requiring students to disclose more personal data than is reasonably necessary to participate in an online educational activity.

- Microsoft entered into a federal court order to resolve FTC allegations that it violated the COPPA Rule when it collected personal information from children who signed up for the Xbox gaming system without notifying parents or obtaining parents' consent. The complaint also alleged that Microsoft retained children's personal information beyond what was allowable under COPPA. The federal court order makes clear that children's avatars, biometric data, and health information are not exempt from COPPA. The order requires Microsoft to inform parents who did not create a child account that doing so will provide additional privacy protections for their child by default. Microsoft must also notify video game publishers when it discloses personal information from children that the user is a child, which providers those publishers notice to apply COPPA's protections to that child. In addition, Microsoft paid a $20 million civil penalty for the COPPA Rule violations.

- WW International, Inc., formerly known as Weight Watchers, and its subsidiary Kurbo, Inc., entered into a federal court order to resolve FTC allegations that these companies violated the COPPA Rule by (a) marketing a weight loss app for use by children as young as eight and then collecting their personal information without getting their parents' verifiable consent and (b) retaining children's personal information indefinitely and only deleting it when requested by a parent. The stipulated order requires the companies to retain data collected from children under 13 for no more than a year after the last time a child uses the app, comply with the COPPA Rule moving forward, and pay a $1.5 million civil penalty. The stipulated order also requires the companies to destroy all personal information previously collected that did not comply with the COPPA Rule's parental notice and consent requirements, unless the companies obtained subsequent parental consent for retaining the data, and to destroy any affected work product that used the data.

- Advertising platform OpenX entered into a stipulated order to resolve FTC allegations that it collected information about children in violation of COPPA. OpenX operates a real-time bidding platform that monetizes websites and mobile apps by selling ad space. The complaint alleged OpenX had knowledge that apps in its ad exchange were child-directed and that it was collecting personal information from children under 13 in violation of COPPA. In addition, the complaint alleged OpenX collected geolocation data from users who opted out of being tracked. The order requires OpenX to delete all ad request data it collected to serve targeted ads, implement a comprehensive privacy program to ensure it complies with COPPA and stops collection and retention of personal data of children under 13, and pay a $2 million civil penalty.

- In a complaint filed by the Department of Justice on behalf of the FTC, the Commission alleged that the operators of the coloring book app Recolor (Kuuhuub Inc., along with its subsidiaries Kuu Hubb Oy and Recolor Oy) collected personal information from children under the age of 13 who used the app's social media features and allowed third-party advertising networks to collect personal information from users in the form of persistent identifiers for targeted ads, in violation of the COPPA Rule. As part of the settlement, the companies agreed to notify users of the app about the alleged COPPA Rule violations, delete personal information they illegally collected from children under the age of 13, offer refunds to current paid subscribers who were underage when they signed up for the app, and pay a $3 million monetary penalty, which was suspended upon payment of $100,000 due to their inability to pay the full amount.

Data Security

Since 2000, the FTC has brought **89 cases** against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data. The FTC continues to strengthen the relief it obtains in data security cases to provide more protection for consumers and accountability for businesses, including data minimization. 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.

- Global Tel*Link, a company that contracts with jails, prisons, and similar institutions to provide services such as communications and payment services for incarcerated individuals, and two of its subsidiaries recently settled with the FTC to resolve allegations that they failed to implement adequate security safeguards to protect consumers' personal information, which resulted in a breach that affected hundreds of thousands of users of their services. The FTC alleged that Global Tel*Link and the two subsidiaries misrepresented their security practices and failed to alert those affected by the breach. The FTC's order requires the entities to implement a

comprehensive data security program with strong safeguards; notify users affected by the breach who did not previously receive notice and provide them with credit monitoring and identity protection products; and notify affected consumers and jails, prisons, and similar institutions within 30 days about future data breaches that trigger any federal, state, or local breach reporting requirements.

- The FTC took action against the online alcohol marketplace Drizly and its CEO James Cory Rellas over allegations that the company's security failures led to a data breach exposing the personal information of about 2.5 million consumers. The FTC alleged that Drizly and Rellas were alerted to security problems two years prior to the breach yet failed to take steps to protect consumers' data from hackers. The FTC's order requires the company to destroy unnecessary data, restricts the consumer data that the company can collect and retain, and binds Rellas to specific data security requirements for his role in presiding over unlawful business practices.

- Chegg, an edtech provider that offers homework help, textbook rentals, online tutoring, and scholarship application assistance, settled with the FTC to resolve allegations that it collected sensitive information about its users and employees, but failed to properly protect this data, leading to several data breaches that exposed the personal data of millions of consumers. The exposed personal information included names, email addresses, passwords, and for certain users, sensitive scholarship data such as dates of birth, parents' income range, sexual orientation, and disabilities. The order requires Chegg to implement a comprehensive data security program with strong safeguards, including documenting and following a data collection and retention schedule, providing multifactor authentication or another authentication method to its customers and employees, and providing customers with access and deletion rights for the information that Chegg collects about them.

- The Commission took action against CafePress for failing to secure consumers' sensitive personal data and covering up a major breach. In its complaint, the Commission alleged that CafePress stored Social Security numbers and password reset answers in clear, readable text; retained the data longer than was necessary; and failed to apply readily available protections against well-known threats and adequately respond to security incidents. As a result of these failures, CafePress's network was breached multiple times, according to the Commission's complaint. Even after it became aware of these breaches, CafePress delayed in notifying consumers and continued to charge them account-closing fees. The Commission's order required the company to bolster its data security, including by upgrading its authentication measures and minimizing the amount of data it collects and maintains; and required its former owner to pay a half-million dollars to compensate small businesses.

- The Commission settled an action against the movie subscription service MoviePass, Inc. and the company's two principals related to the company's failure to secure subscribers' data, and the tactics the company took to prevent subscribers from using the service as advertised. According to the Commission's complaint, MoviePass advertised that consumers could see "one movie per day" for a monthly rate of $9.95. However, MoviePass stifled subscribers' ability to use the service, including by invalidating subscriber passwords, requiring that subscribers verify their movie tickets, and employing "trip wires" that blocked certain frequent users from utilizing the service. MoviePass also failed to take reasonable steps to secure personal information it collected from subscribers. For example, the company stored consumers' personal data, including financial information and email addresses, in plain text and failed to impose restrictions on who could access personal data. The Commission order against MoviePass, its parent company, and its two principals bars the respondents from misrepresenting their business and data security practices and requires that they implement comprehensive information security programs.

- A federal court entered an order against Ring, resolving FTC allegations that the maker of connected home security cameras had illegally surveilled customers in private spaces of their homes and had failed to take reasonable steps to prevent hackers from gaining access to customer accounts, live streams of videos, and stored videos. Among other relief, the order also requires Ring to implement a privacy and security program with novel safeguards on human review of videos as well as other stringent security controls, such as multi-factor authentication for both employee and customer accounts. The order requires independent assessments of that program.

- The FTC alleged that Twitter (now X) deceptively used Twitter users' phone numbers and email addresses (which Twitter claimed were collected for security purposes) for targeted advertising from 2014 to 2019, in violation of both Section 5 and a previous Commission order against the company. Users provided phone numbers or email addresses to Twitter for a variety of security purposes, such as for two-factor authentication or to unlock an account where Twitter detected suspicious or malicious activity. The FTC alleged that Twitter would then use this contact information to allow advertisers to target specific groups of Twitter users by matching the telephone numbers and email addresses that Twitter collected to the advertisers' lists of telephone numbers and email addresses, or to import marketing lists from data brokers for matching purposes. Among other things, the stipulated order required Twitter to pay a $150 million civil penalty. A novel feature of the order is the requirement that Twitter must allow its users to take advantage of multi-factor authentication choices that do not require providing Twitter a phone number, such as mobile authentication apps or security keys.

Credit Reporting & Financial Privacy

The FTC protects consumers' financial privacy and upholds safeguards for credit reporting, through enforcement of Section 5 of the FTC Act and several specific laws that govern the handling and use of data in the financial sectors. 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 **117 cases** against companies for violating the FCRA and has obtained **more than $137 million in civil penalties**. These cases have helped ensure 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 Act (GLB) as implemented in the CFPB's Regulation P and the FTC's Privacy Rule, 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. The FTC Safeguards Rule 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.[4] From 2021 to 2023, the FTC brought the following credit reporting and financial privacy cases:

- TransUnion Rental Screening Solutions and its parent, Trans Union LLC, entered into a stipulated order to resolve the Commission's and CFPB's allegations that they violated the FCRA. The FTC's and CFPB's joint complaint alleges that the companies failed to use reasonable procedures to ensure the accuracy of eviction records they included in tenant screening reports, by making consumers' eviction histories look more extensive than they were, reporting inaccurate or incomplete outcomes, mischaracterizing amounts they reported with eviction records, and failing to prevent sealed eviction records from being included in the reports. The complaint also alleges the companies failed to disclose the sources of their public records, as required by the FCRA, because they did not name the vendors from which they directly acquired those records. The order requires the companies to pay $11 million in consumer redress to certain consumers affected by their practices and a $4 million civil penalty. It also requires the companies to make changes to fix their unlawful practices, including designing procedures to prevent the inclusion of certain incomplete, misleading, or sealed eviction records. The order also requires the companies to take steps to help consumers learn what is on their tenant screening reports and why landlords have taken adverse actions against them.

[4] Relatedly, the FTC also enforces the Fair Debt Collection Practices Act (FDCPA), which 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.

- Background check companies TruthFinder and Instant Checkmate and their affiliates entered into a stipulated order to resolve allegations that they violated the FCRA and Section 5. The complaint alleges the companies operated as consumer reporting agencies within the scope of the FCRA because, among other things, they marketed their reports for employee and tenant screening using Google Ads keywords, but the companies failed to comply with FCRA requirements, such as using reasonable procedures to ensure the maximum possible accuracy of their consumer reports. The complaint also alleges the companies violated Section 5 by making deceptive representations about whether consumers had criminal records and whether consumers had been compensated for posting reviews of the companies' products. The order requires the companies to implement policies and procedures to assess and monitor whether they are operating as consumer reporting agencies, to follow the FCRA if so, to monitor whether consumer reviewers and other endorsers are properly disclosing any compensation or benefit received from the companies, to refrain from making misrepresentations to consumers, and to pay a $5.8 million civil penalty for the FCRA violations.
- Lead generation company ITMedia Solutions Inc. entered into a stipulated order to resolve FTC allegations that ITMedia, a number of affiliate companies, and their owners and officers operated hundreds of websites that were designed to entice consumers into sharing their most sensitive financial information under the guise of connecting them with lenders. The defendants sold consumers' sensitive information to marketing companies and others without regard for how the information would be used, according to the complaint. The complaint alleged that ITMedia violated the FCRA by unlawfully obtaining and reselling the credit scores of consumers who submitted information. ITMedia agreed to pay a $1.5 million civil penalty for the FCRA violations.
- Smart home security and monitoring company Vivint Smart Home, Inc. agreed to pay $20 million to settle FTC allegations that Vivint violated the FCRA by improperly obtaining credit reports to qualify potential customers for financing. The FTC alleged that some Vivint sales representatives used a process known as "white paging," which involved finding another consumer with the same or a similar name on the White Pages app and using that consumer's credit history to qualify the prospective unqualified customer. In addition to the record-setting $20 million FCRA monetary judgment, this was the FTC's first law enforcement action brought under the Red Flags Rule. The settlement requires Vivint to implement an employee monitoring and training program, as well as an identity theft prevention program. The company must also establish a customer service task force to verify that accounts belong to the right customer before referring any account to a debt collector and must assist consumers who were improperly referred to debt collectors.
- The Commission is currently in litigation with a bogus credit repair company that, when seeking to obtain consumers' credit reports from consumer reporting agencies, made false certifications as to its permissible purpose in violation of FCRA. The FTC's amended complaint in FTC v. Financial Education Services

alleges that the company preys on consumers with low credit scores by luring them in with the false promise of an easy fix and then recruiting them to join a pyramid scheme selling the same worthless credit repair services to others. The company claims to offer consumers the ability to remove negative information from credit reports and increase credit scores by hundreds of points, charging as much as $89 per month for their services. Their techniques, according to the complaint, are rarely effective and in many instances harm consumer's credit scores.

Spam Calls and Email

The FTC vigorously enforces federal laws that give consumers the right to be left alone from unwanted telemarketing and email marketing.

Do Not Call Cases

In 2003, the FTC amended the Telemarketing Sales Rule (TSR) to create a national Do Not Call (DNC) Registry, which now includes more than **249 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. In many instances, these calls are the springboard for deceptive sales pitches that result in substantial monetary losses.

Since 2003, the FTC has brought **167 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 557 companies and 443 individuals involved. The 157 cases concluded thus far have resulted in orders totaling more than $2.1 billion in civil penalties, redress, or disgorgement, and actual collections exceeding $395 million. These actions have halted billions of abusive and fraudulent calls that invade consumers' privacy and cause significant economic harm.

The FTC shut down more than a billion robocalls through a sweep, "Operation Stop Scam Calls." Many of these cases alleged that the defendants tricked consumers into providing personal information and "consent" to receive robocalls.

- In Fluent, LLC, the FTC sued a second consent farm. The defendants' operations obtained purported consent from nearly one million consumers a day, and between January 2018 and December 2019, the defendants sold more than 620 million leads. The defendants lured consumers through two different types of misleading websites. The first were "reward sites" that offered consumers valuable items such as cash awards and gift cards. Defendants and the third-party publishers that defendants worked with told consumers that the rewards were "free" or "fast and easy" to obtain. The second were job websites that told

consumers that high paying jobs with attractive benefits were available. When consumers visited these websites and provided their contact information either to "register" for a reward or apply for a job, they purportedly consented to receive live calls and robocalls from dozens or even hundreds of third parties. The FTC sued defendants for misrepresenting the terms of its offers, assisting and facilitating telemarketing violations, and violating the CAN-SPAM Act by sending emails with misleading header and subject information. To settle the lawsuit the defendants agreed to pay $2.5 million. Defendants also agreed to extensive injunctive relief including providing clear and conspicuous disclosures when it obtains consumers' contact information, vetting the third parties it works with, and a ban on making robocalls.

- In Yodel Technologies, Inc. the FTC sued an operator of "soundboard" technology whose clients made millions of robocalls to consumers. Soundboard technology allows call center agents to play pre-recorded audio clips using "response keys" to engage consumers. The pre-recorded clips asked automated questions like "Can you hear me okay" and engaged in other tactics that were part of a sales pitch intended to keep consumers on the line until the call could be transferred to one of Yodel's clients. Yodel made more than 1.4 billion calls to U.S. consumers, and it used soundboard technology in all or a substantial amount of these calls. At times, Yodel initiated more than 2.5 million calls in a single day. Yodel often purchased the contact information of consumers from "consent farms" like Viceroy Media, whom the FTC also sued. The consent farms engaged in deceptive practices to trick consumers into purportedly consenting to receive prerecorded calls from dozens or hundreds of third-parties. Yodel then purchased the contact information of these consumers and bombarded the consumers with robocalls on behalf of its third-party clients. Yodel agreed to a permanent ban on telemarketing, and to a $1 million judgment. Yodel paid $400,000 and the remainder of the judgment was suspended due to an inability to pay.

- In Viceroy Media Solutions, the FTC sued a group of defendants that operated a "consent farm" that resulted in consumers receiving unlawful calls. The defendants ran the websites quick-jobs.com and localjobsindex.com. Consumers seeking jobs would visit the websites and provide their contact information to receive job updates. When consumers clicked "continue" they purportedly agreed to a privacy policy in which they consented to receive marketing calls and robocalls from up to 90 "partners." The defendants sold the consumers' information as contact leads to these partners, and the partners would then inundate consumers with unwanted calls. The defendants sold more than 45 million leads in a three-year period. The FTC sued the defendants for assisting and facilitating the unlawful calls made by the partners because the defendants did not obtain meaningful consent from consumers and because the TSR requires sellers to obtain consent directly from consumers to place robocalls, not through intermediaries like Viceroy. The defendants agreed to a ban on making or assisting others in making robocalls. They also agreed to provide clear and conspicuous disclosures on their employment websites when they were

collecting consumer information that they would sell to third-parties. The defendants paid $150,000 to settle the case. The remainder of the $900,000 judgment was suspended due to an inability to pay.

- In Solar Xchange LLC, the FTC and the State of Arizona sued two groups of defendants for making unlawful telemarketing calls in connection with the sale of solar panels. The Solar Xchange defendants contacted consumers to try to set up appointments for Vision Solar representatives to pitch solar panels. Solar Xchange placed tens of millions of calls to consumers on the DNC list, thousands of whom received dozens of calls. Solar Xchange agreed to an order that would prohibit it from engaging in deceptive conduct and that would require it to vet its lead generators and ensure they are not engaged in deceptive practices. The order also included a $13 million judgment. Solar Xchange paid $62,500 and the remainder of the judgment was suspended due to an inability to pay. The complaint alleges that Vision Solar falsely claimed an affiliation with utility companies or government agencies and that it misrepresented the amount of money consumers could save. Litigation against Vision Solar is ongoing.

- In Hello Hello Miami, LLC, the FTC sued a VoIP provider and its owner for assisting and facilitating the transmission of approximately 37.8 million illegal robocalls on behalf of more than 11 different foreign telemarketers. According to the complaint, of those calls, approximately 52% were delivered to U.S. customers on the Do Not Call Registry. The robocalls at issue delivered a pre-recorded message that falsely claimed to be from Amazon. Many of the calls alerted the customer that their Amazon account was on hold, that the customer had experienced a suspicious charge, or the customer's Amazon account was about to be renewed. These calls were not authorized by Amazon and Hello Hello Miami repeatedly received notice that providers were using their services to transmit these types of illegal robocalls. The district court entered a default judgment against Hello Hello Miami. The judgment requires Hello Hello Miami to take steps to screen and monitor its current and prospective customers.

In addition to Operation Stop Scam Calls, the Commission initiated actions and settled or obtained judgments for other DNC violations as described below:

- In Benefytt Technologies, Inc., the FTC sued a network of defendants that sold consumers sham health care products. Defendants and their distributors claimed that the products defendants sold were health insurance and that the provided coverage was equivalent to or provided the benefit of a "qualified health plan" under the Affordable Care Act. Many consumers learned the truth about Benefytt's products only when they needed the benefits defendants promised, such as trying to schedule an appointment with a doctor or fill a prescription. Some consumers incurred hundreds or thousands of dollars of medical debt under the false assumption that the expenses would be covered. Defendants and their distributors marketed their products in part through outbound telemarketing to numbers on the Do Not Call Registry and by using prerecorded messages. To settle the charges, Benefytt agreed to pay $100 million to provide refunds to

consumers harmed by Benefytt's practices. Benefytt also agreed to inform its customers of the FTC's actions, provide refunds, and allow customers to cancel their plans. Benefytt also agreed to avoid misleading consumers in the future and to closely monitor the companies it uses to sell its products.

- In Associated Community Services, Inc., the FTC and 46 agencies from 38 states and the District of Columbia stopped a telefunding operation that bombarded 67 million consumers with 1.3 billion deceptive charitable funding calls, most of which were robocalls. The defendants collected more than $110 million using deceptive solicitations. The defendants claimed that the money they collected would go to organizations that helped breast cancer patients, families of children with cancer, and homeless veterans, among other causes, but in fact defendants and their nonprofit clients kept almost all of the money raised, using almost none of the $110 million collected to help the charitable causes ACS described to donors. Most of the defendants were permanently banned from conducting any fundraising activity or telemarketing for any kinds of goods or services. The defendants were ordered to pay $100 million, which was partially suspended due to an inability to pay. The defendants paid $500,000.

- In Environmental Safety International, Inc., the FTC sued the operators of a company that sells septic tank cleaning products. The defendants initiated more than 45 million illegal telemarketing calls to consumers that purported to provide "free info" on a septic tank cleaning product. Consumers were then subject to a sales pitch. The defendants agreed to a ban on telemarketing and paid more than $1.65 million.

- In American Vehicle Protection Corp., the FTC sued a group of entities that sold extended automobile warranties. Defendants called consumers on the Do Not Call Registry and falsely claimed to be affiliated with the consumers' auto company. Defendants also told consumers that the warranties provided "bumper-to-bumper" coverage, and consumers could receive a full refund if they were not satisfied within 30 days. These claims were all false. Defendants had no affiliation to auto companies, the warranties had extensive limitations, and defendants made it very difficult for consumers to obtain refunds. The primary defendants agreed to a lifetime ban on outbound telemarketing, and from any future involvement in extended automobile warranty sales. They also agreed to pay $500,000 of a stipulated $6.6 million monetary judgment, which was partially suspended due to an inability to pay.

- In XCast Labs, Inc.,the FTC sued a VoIP provider responsible for delivering billions of illegal robocalls to consumers. The robocalls included robocalls claiming affiliation with government entities such as the Social Security Administration, robocalls threatening to cut off a call recipient's utility services, and calls claiming that the recipients' credit card has been charged and they must act promptly for a full refund. The Industry Traceback Group sent XCast over 100 traceback requests, which are messages to XCast seeking information about the source of suspicious traffic XCast routed. Many of the requests

expressly noted that the calls were fraudulent. XCast also received complaints from other sources about the traffic it routed, including a 2020 warning letter from the FTC. XCast continued routing traffic for customers whom it knew were transmitting suspicious or illegal calls. Xcast agreed to a stipulated order requiring it to follow the law, refrain from doing business with high-risk customers, and screen its clients. The order also includes a $10 million penalty which was suspended due to an inability to pay.

- In Home Matters USA, the FTC and the California Department of Financial Protection and Innovation sued the operators of a mortgage loan modification scheme. Defendants told consumers that in three months they would substantially reduce the consumers' mortgage payments and the total amount they were required to pay. Defendants also implied that they were associated with government relief programs, including COVID-19 relief programs. Defendants marketed their programs in part by calling consumers on the Do Not Call Registry. The FTC obtained a temporary restraining order halting the defendants' business operations. The litigation is ongoing.

- In Stratics Networks Inc., the FTC sued seven corporate and five individual defendants for various TSR violations, including placing illegal calls to consumers and charging advance fees for debt relief services. Defendant Stratics Networks claimed to be the "U.S. Inventor[] of Ringless Voicemail" and offered a platform where its customers could purportedly deliver a pre-recorded message directly to the consumers' voicemail box without causing the phone to ring. Some telemarketers believe that consumers are more likely to listen to a voicemail message than they are to answer an incoming call from an unknown number. Stratics also offered more traditional robocall services. Stratics' customers robocalls pitched a variety of goods and services, including homebuying services, credit card and student debt relief, and health insurance. The FTC also sued a group of defendants known as the Atlas Defendants who sold debt relief services using Stratics' ringless voicemail platform. The Atlas Defendants placed more than 23 million robocalls using Statics' ringless voicemail platform without the recipients' prior express written consent to receive prerecorded messages. Atlas, and its fulfillment partner, Ace Business Solutions, charged consumers upfront fees for debt relief services in violation of the TSR. A marketing contractor for the Atlas Defendants, Kasm, and its owner, agreed to a stipulated order that would require them to follow the law and vet the lead generators they used to recruit customers. Defendant Netlatitude, also a customer of Stratics, and its individual owner, agreed to a stipulated order requiring them to follow the law and better screen its telemarketing customers. Litigation against Stratics, the Atlas Defendants, and Ace Business Solutions is ongoing.

- In VOIP Terminator, Inc., the FTC sued a VoIP provider and the firms' owners for assisting and facilitating the transmission of millions of illegal prerecorded telemarketing calls including calls that offered an air duct cleaning service that purportedly helped stop the transmission of COVID-19. The defendants agreed to an order that prohibits them from violating the Telemarketing Sales Rule and

requires them to review all current and prospective clients to make sure that they are not engaged in deceptive acts or practices.

CAN-SPAM

The FTC brought two cases under the CAN-SPAM Act, which protects consumers from receiving commercial email they consider to be spam.

- In a complaint against ConsumerInfo.com d/b/a Experian Consumer Services ("Experian"), the FTC alleged that the company spammed consumers who signed up for an account with the company with marketing emails they could not opt out of, in violation of the CAN-SPAM Act. Creating an account with Experian is required for consumers to be able to manage their Experian credit information online or to implement a credit freeze. The FTC alleged that, despite language in the messages saying that they were "important updates" about a consumer's account, the emails were in fact marketing messages promoting company products and services as well as third-party offers. The CAN-SPAM Act requires marketing emails to contain a clear and conspicuous notice of consumers' right to opt out of receiving further marketing emails and a way for them to do so, which these messages did not. A settlement agreement filed by the Department of Justice on behalf of the FTC prohibits Experian from sending marketing messages without an opt-out mechanism and required it to pay a $650,000 civil penalty.

- In its complaint against Publishers Clearing House (PCH), the FTC alleged that PCH used deceptive dark patterns to trick consumers into buying products to enter or increase their odds of winning one of the company's sweepstakes. In truth, consumers did not need to make any purchases to enter or to increase their odds of winning a sweepstakes. PCH also sent emails to consumers with misleading subject headings, like "High Priority Doc. W-2 Issued" and "CONFIRMED & BINDING Contents Re. Doc W11," that created a false sense of urgency for recipients to open and click on links in the messages. In addition to charging PCH with violations of the CAN-SPAM Act for its use of deceptive email subject headings, the FTC alleged that PCH violated the FTC Act by misrepresenting to consumers that it would not sell their data to third parties, even though the company did just that until January 2019. Under a settlement agreement, PCH was required to make a number of key changes to its email and internet operations, including stopping the practice of deceiving consumers about purchases and sweepstakes, making clear disclosures, stopping deceptive emails, and destroying consumer data it collected before January 2019. In addition, PCH paid $18.5 million to the Commission to be used to refund consumers.

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 EU-U.S. Data Privacy Framework (DPF).[5] This new Framework, provides a mechanism for companies to transfer personal data from the EU to the United States consistent with EU law. To join the Data Privacy Framework, a company must self-certify to the Department of Commerce that it complies with the Data Privacy Framework Principles. A company's failure to comply with the Principles is enforceable under Section 5, prohibiting unfair and deceptive acts or practices. The FTC, in a letter from Chair Lina Khan, has committed to vigorous enforcement of the DPF Principles, and will work with privacy authorities in the EU to protect consumer privacy on both sides of the Atlantic.

Overall, the FTC has brought **69 actions** to enforce companies' promises under these international privacy programs: 39 under the Safe Harbor program, 4 under APEC CBPR, and 26 under Privacy Shield. Since January 2021, the FTC resolved the following matters, described above, arising under the Privacy Shield Framework:

- In Flo Health, the FTC alleged that the fertility-tracking app disclosed user health information to third-party data analytics providers after promising to keep such information private. The FTC complaint specifically notes the company's interactions with EU consumers and alleges that Flo violated EU-U.S. Privacy Shield Principles 1 (Notice), 2 (Choice), 3 (Accountability for Onward Transfer), and 5 (Data Integrity and Purpose Limitation).

- In CafePress, the FTC alleged that the company failed to secure consumers' sensitive information, covered up a major data breach, and violated EU-U.S. Privacy Shield Principles 2 (Choice), 4 (Security), and 6 (Access).

- In Twitter, the FTC secured $150 million from Twitter for its violation of an earlier FTC order with practices affecting more than 140 million customers, including violating EU-U.S. Privacy Shield Principle 5 (Data Integrity and Purpose Limitation).

ARTIFICIAL INTELLIGENCE

As highlighted above, the Commission has brought numerous law enforcement actions against companies whose use of artificial intelligence compromised the privacy of consumers' sensitive personal information. For example, in the Rite Aid Corp. and Amazon/Alexa matters, the Commission alleged that the companies engaged in unfair practices related to the use of facial recognition and voice recognition technologies

[5] The Data Privacy Framework replaces the EU-U.S. Privacy Shield Framework (and its predecessor program, the U.S.-EU Safe Harbor Framework). On July 10, 2023, the European Commission issued an adequacy decision on the Data Privacy Framework. Other international data frameworks have included the Swiss-U.S. Privacy Shield Framework and the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules System (APEC CBPRs).

(respectively). In the Everalbum, Inc. and Ring matters, the Commission alleged that the companies misled consumers about how their photos or videos (respectively) would be used; according to the FTC's complaints, consumers did not know that the companies would use their data to develop image recognition technology. In these settlements, as well as in the settlements described above with Weight Watchers and CRI Genetics, the Commission's orders have required companies to delete data product (algorithms and other tools) developed from unlawfully obtained data. The "Hey, Alexa!" business guidance from Commission staff described above has highlighted the privacy implications of using consumer data to power AI.

In addition to these law enforcement actions,[6] the Commission has engaged in numerous other actions—settlements, reports, policy statements, workshops—related to artificial intelligence since January 2021.

- In response to a statutory direction, the Commission issued Combatting Online Harms Through Innovation: A Report to Congress. This 78-page report discussed the use of AI to detect or otherwise address a wide variety of harmful online content. The report described the various ways that automated tools are or could be used to help in such efforts, but it cautioned that these tools often have limited success and suffer from severe shortcomings that militate against promoting or over-relying on their use with respect to many of the harms. The report also discusses legislation to advance platform transparency and accountability.

- As part of an ongoing market study, the FTC issued orders under Section 6(b) of the FTC Act to eight social media and video streaming platforms seeking information on their use of automation and human review to limit consumer exposure to paid advertising for fraudulent health-care products, financial scams, counterfeit and fake goods, or other fraud. The orders also seek information about whether and how companies use algorithmic, machine learning, or

[6] In addition to the settlements described above at the nexus between privacy and AI, the FTC has settled other matters in which companies allegedly made deceptive promises about investments or business opportunities based on the supposed efficacy of an AI or algorithmic tools. In WealthPress, the defendants had to refund more than $1.2 million to consumers and pay a $500,000 civil penalty because of false earnings claims. According to the FTC's complaint, defendants represented their purported expert leveraged his extensive expertise to develop an algorithm or strategy that consistently identifies extremely profitable trades, and that consumers would generate substantial trading profits when they used the algorithm. Instead, consumers lost substantial sums of money when investing based on defendants' trade recommendations. The case marked the FTC's first collection of civil penalties against a company that received the agency's Notice of Penalty Offenses regarding money-making opportunities sent in October 2022, and the first civil penalties for violations of the Restore Online Shoppers' Confidence Act (ROSCA). In DK Automation, defendants had to turn over $2.6 million to refund consumers harmed by empty promises of big returns on an Amazon business opportunity scheme generated by a "fully automated, fully-automatic algorithm." And in Automators AI, the FTC obtained a temporary restraining order against defendants claiming that its AI-boosted tools would power high earnings through online stores. A stipulated preliminary injunction was signed by the court on September 8, 2023.

automated systems, including generative artificial intelligence systems, to create and optimize paid content.

- Chair Khan joined leaders of the Department of Justice's Civil Rights Division, the Equal Employment Opportunity Commission, and the Consumer Financial Protection Bureau to issue a "Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems."

- The FTC issued a policy statement, discussed in more detail below, explaining the application of Section 5 to the collection and use of biometric information and technologies that process biometric information. Such technologies often rely on machine learning or similar techniques.

- The FTC started the Voice Cloning Challenge, an open, exploratory challenge to the public to develop multidisciplinary approaches—from products to policies to procedures—aimed at protecting consumers from AI-enabled voice cloning harms, such as fraud and the broader misuse of biometric data and creative content. Submissions that are able to address harms, as defined by the judging criteria, will be eligible for challenge prizes that can be used to further develop and implement the given solution. The Challenge encourages individuals, teams of individuals, and organizations to develop and submit ideas aimed at protecting consumers from AI-enabled voice cloning harms, such as fraud and the broader misuse of biometric data and creative content. Submissions must, at a minimum, address one or more of the following voice cloning harms intervention points: (1) Prevention or Authentication - Methods to limit the use and application of voice cloning software by unauthorized users; (2) Real-time Detection or Monitoring - Methods to detect cloned voices or the use of voice cloning technology; or (3) Post-use Evaluation - Methods to check after the fact if audio clips contain cloned voices.

- The FTC's PrivacyCon is a recurring event, open to the public, that features panels and presentations by researchers and experts relating to consumer privacy, data security, and emerging technologies. Recent iterations of PrivacyCon have included significant discussion of AI, such as a 2021 panel on algorithms and a 2022 panel discussion on automated decision-making systems.

- The FTC held a virtual roundtable on AI and content creation. The event focused on the impact of generative AI on creative fields and featured comments from representatives of a variety of those fields. The following month, the Commission submitted a formal comment to the U.S. Copyright Office raising competition and consumer protection concerns about generative AI and stressing that it will use its authority to combat potential harm to consumers, workers, and small businesses.

- In addition, Commission staff have published business guidance highlighting the consumer protection and competition issues related to AI. In 2021, FTC staff issued a business blog post entitled "Aiming for truth, fairness, and equity in your company's use of AI." This post highlights some of the laws enforced by the FTC that could apply to developers and users of AI, including Section 5 of the FTC Act, the Fair Credit Reporting Act, and the Equal Credit Opportunity Act. It provides seven principles that businesses developing or using AI should follow (such as embracing transparency, independence, and accountability) and warns that discriminatory outcomes could be unfair. This post makes clear that the FTC will not hesitate to hold companies accountable for law violations related to the development or use of AI.

- The FTC issued five business blog posts in 2023 as part of its "AI and Your Business" series and a sixth business blog post on AI and data collecting, highlighting lessons on AI from the Amazon/Alexa and Ring matters. These posts included cautions that companies should not make unsupported or exaggerated claims about the capabilities of AI tools, could be liable for offering generative AI tools that are used to deceive others or that manipulate consumers into unintended decisions, and should watch out for deceptive claims that a tool can reliably detect AI-generated content. The last post explored issues regarding digital ownership and creation, such as passing off AI-generated content as the work of real artists or writers, and the potential liability of companies for not coming clean about the extent to which the output of their generative AI tools may reflect the use of copyrighted or otherwise protected material.

- The FTC's Office of Technology issued blog posts relating to AI, one with the Bureau of Competition exploring competition issues such as market concentration, and one exploring consumer concerns about AI per an analysis of the FTC's complaint database.

- The FTC issued consumer alerts regarding AI-related scams. One of them cautioned people about how scammers are using AI to enhance family emergency schemes, and the other discussed advertisements for fake AI tools that spread malicious software.

RULES

Congress has authorized the FTC to issue rules that regulate specific areas of consumer privacy and security. In addition, Section 18 of the FTC Act (15 U.S.C. §57a) governs the Commission's authority to promulgate rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce (Magnuson-Moss Rules). Since 2021, the FTC's rulemaking activity related to privacy and data security has included the following.

- 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 December 2021, the Commission issued an amended Privacy Rule and an amended Safeguards Rule, which became effective on June 9, 2023. In October 2023, the Commission issued a breach notification amendment to the GLB Safeguards Rule, which requires financial institutions to notify the FTC of breaches affecting 500 or more consumers.

- 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 June 2023, the Commission issued a Notice of Proposed Rulemaking to strengthen and modernize the Rule, including by clarifying its application to health apps and similar technology. During the public comment period, which closed in August, the FTC received 128 comments, which the Commission is now considering.

- The COPPA Rule requires websites and online services to get parental consent before collecting, using, or disclosing personal information from children under 13. In 2019, as part of its ongoing effort to ensure that the COPPA Rule is 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. In December 2023, the Commission issued a Notice of Proposed Rulemaking to strengthen the COPPA Rule and address the evolving ways personal information from children is being collected, used, and disclosed. The public had until March 11, 2024, to submit a comment on the proposed changes to the COPPA Rule.

- Commercial Surveillance and Data Security Rulemaking. In August 2022, the FTC announced it is exploring rules, under its Magnuson-Moss rulemaking authority, to crack down on harmful commercial surveillance and lax data security. Commercial surveillance is the business of collecting, analyzing, and profiting from information about people. Mass surveillance has heightened the risks and stakes of data breaches, deception, manipulation, and other abuses. The FTC's Advance Notice of Proposed Rulemaking sought public comment on the harms stemming from commercial surveillance and poor data security practices, and whether new rules are needed to protect people's privacy and information. Comments closed in November 2022; staff is currently reviewing more than 10,000 comments.

Other Rules that Regulate Specific Areas of Consumer Privacy and Security

- 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 retain the CAN-SPAM Rule without change.

- Under the FCRA, the Red Flags Rule requires financial institutions and certain creditors to have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft. The Commission brought its first law enforcement action under the Rule in its case against Vivint. 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 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.

POLICY STATEMENTS AND OTHER ACTIONS

Since 2021, the Commission has issued policy statements, sent warning letters, and issued a notice of penalty offense relating to privacy and data security.

Notice of Penalty Offenses Concerning Misuse of Information Collected in Confidential Contexts to Tax Preparation Companies (September 2023). The Commission issued a notice of penalty offense ("NPO") describing several unfair and deceptive practices related to the misuse of information where a consumer reasonably expects that such

information will remain confidential. The notice warns against using such information: (a) for purposes not explicitly requested by the individual; (b) to obtain a financial benefit that is separate from the benefit generated from providing the product or service requested by the individual; and (c) to advertise, sell, or promote products or services. The Commission further noted that it is unlawful to make false, misleading, or deceptive representations concerning the use or confidentiality of such information. In conjunction with the NPO, the Commission sent letters to five tax preparation companies warning that they could incur civil penalties if they misuse tax return information or other confidential data in ways that run counter to the original purpose for which the information was collected. The letters specifically warned against the use of tracking technologies like pixels and cookies to amass, analyze, infer, or transfer confidential information for the above purposes without first obtaining consumers' express consent.

FTC and HHS warning letters on online tracking technologies (June 2023). The FTC and HHS' Office for Civil Rights sent joint letters to approximately 130 hospital systems and telehealth providers cautioning them about the associated privacy and security risks related to the use of online tracking technologies, such as the Facebook/Meta pixel, integrated into their websites or mobile apps that may be impermissibly disclosing consumers' sensitive personal health data to third parties. These tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app.

Biometric Policy Statement (May 2023). The Commission issued a policy statement warning that the increasing use of consumers' biometric information and related technologies, including those powered by machine learning, raises significant consumer privacy and data security concerns and the potential for bias and discrimination. The statement discusses new and increasing risks that consumers face associated with the collection and use of biometric information, including risks that: biometric information can be used to create deepfakes that can be used for fraud or harassment; large databases of biometric information may be a target for malicious actors; the technologies may be used to identify consumers in certain locations, revealing sensitive information about them; and that some technologies using biometric information, such as facial recognition technology, may perform differently across different demographic groups in ways that facilitate or produce discriminatory outcomes. The statement makes clear that though many biometric information technologies are new, businesses must continue to abide by longstanding legal requirements and obligations and lists examples of practices the Commission will look at in determining whether a company's use of biometric information or related technologies is deceptive or unfair in violation of Section 5.

Joint Statement on AI with DOJ, CFPB, and EEOC (April 2023). As noted above, Chair Khan joined leaders of the Department of Justice's Civil Rights Division, the Equal Employment Opportunity Commission, and the Consumer Financial Protection Bureau to issue a "Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems."

Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act (May 2022). In response to rising concerns regarding data collection through education technology, the Commission issued a policy statement on Ed Tech and COPPA. The statement addresses COPPA's application in the online learning context and makes clear that COPPA prevents Ed Tech companies from denying children access to their services when parents or schools refuse to agree to commercial surveillance. In addition, the statement underscores that Ed Tech providers must comply fully with all provisions of the COPPA Rule, including the prohibition against mandatory collection, limitations on the use of children's data collected pursuant to school authorization, retention limitations, and data security requirements. Finally, the statement notes that the Commission will closely scrutinize Ed Tech providers and will not hesitate to take action against such providers when they fail to live up to their legal obligations to protect children's privacy.

FTC Policy Statement on Enforcement Related to Gig Work (September 2022). The Commission issued a policy statement reinforcing that the FTC will use its full authority to protect gig workers from unfair, deceptive, and anticompetitive practices. The statement noted that internet-enabled "gig" companies have grown exponentially and gig work now composes a significant part of the United States economy. In the gig economy, companies may employ algorithms to govern how gigs are made available to workers, how workers are paid, how worker performance is rated, and when workers are suspended or terminated from the platform. However, companies are responsible for fulfilling their promises to their workers, even if they use automated management technologies. Gig companies that employ algorithmic tools to govern their workforce should ensure that they do so legally.

Statement of the Commission on Breaches by Health Apps and Other Connected Devices (September 2021). The Commission issued a policy statement clarifying that health apps and connected devices that collect or use consumers' health information must comply with the FTC's Health Breach Notification Rule, which requires notification to consumers, the FTC, and, in some cases, the media, of the breach of identifiable health information. The FTC's Health Breach Notification Rule ensures that numerous entities not covered by the Health Insurance Portability and Accountability Act (HIPAA) face accountability when consumers' sensitive health information is breached. The policy statement notes that health apps, which can track everything from glucose levels for those with diabetes to heart health to fertility to sleep, increasingly collect sensitive and personal data from consumers and clarifies the applicability of the FTC's Health Breach Notification Rule to these apps and their data sharing practices.

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.

- The Commission issued 6(b) orders to nine social media companies. The Order was wide-ranging and required them to provide information relating to the impact these services have on U.S. consumers in several important areas, including collection and use of personal and demographic information; methods of determining what ads will be shown to which consumers; application of algorithms and data analytics to personal information; measurement and promotion of user engagement; and how their practices affect children and teens. The orders were sent to Amazon.com, Inc., which operates the Twitch streaming platform; ByteDance Ltd., which operates the short video service TikTok; Discord Inc.; Facebook, Inc.; Reddit, Inc.; Snap Inc.; Twitter, Inc.; WhatsApp Inc.; and YouTube LLC. The purpose of the Order is to collect and compare information about practices across this industry to inform agency policy going forward, and also to inform any future agency report.

- As described in the AI section, above, in March 2023, the Commission also issued orders under Section 6(b) of the FTC Act to eight social media and video streaming platforms seeking information on their use of automation and human review to limit consumer exposure to paid advertising for fraudulent health-care products, financial scams, counterfeit and fake goods, or other fraud.

- The Commission and the CFPB issued a Joint FTC-CFPB Request for Information (RFI) on Tenant Screening solicited comments about housing application and screening practices that may prevent consumers from obtaining or retaining rental housing. The RFI also asked about the harms and benefits of those practices. The Commission and CFPB received comments from all of the categories of stakeholders who play a part in that system, including tenants, advocacy groups, property managers and landlords of all sizes, tenant screening companies, and other members of the public. The FTC may use the information provided for policy development, law enforcement initiatives, and consumer and business education.

- RFI on Cloud Computing. The Commission issued an RFI on the business practices of cloud computing providers, with questions addressing single points of failure, cloud security, generative AI, and market power and competition. In May 2023, the Commission convened a virtual panel of experts to discuss these issues. Staff from the Office of Technology and Bureau of Competition published findings from the RFI and virtual panel in a blog post, and presented these findings at the FTC's November 2023 Open Commission meeting.

- Public Comment on COPPA Rule Parental Consent Application of ESRB. In July 2023, the Commission published for public comment an application from the Entertainment Software Rating Board, Yoti Ltd. and Yoti (USA) Inc., and SuperAwesome Ltd. (collectively "the ESRB Group") that requests the Commission approve a new method for obtaining verifiable parental consent under the COPPA Rule. The ESRB Group calls the proposed method "Privacy-Protective Facial Age Estimation." The applicants submitted the application

pursuant to Section 312.12(a) of the COPPA Rule, which permits interested parties to file a written request for Commission approval of parental consent methods that are not currently enumerated in section 312.5 of the COPPA Rule. The Commission is currently reviewing the application and the more than 350 public comments the Commission received on it.

- The Commission also submitted a FTC Report to Congress on Privacy and Security, in which the Commission provided a comprehensive internal assessment measuring the agency's current efforts related to data privacy and security.

WORKSHOPS

Beginning in 1996, the FTC has hosted approximately 80 workshops, town halls, and roundtables bringing together stakeholders to discuss emerging issues in consumer privacy and security. Recently, the FTC hosted the following privacy events:

PrivacyCon 2022. Following on the success of PrivacyCon 2021 in July 2021, the FTC held the seventh PrivacyCon in November 2022 as a virtual workshop. With almost 2,000 unique viewers in attendance, the sessions focused on research related to Consumer Surveillance, Automated Decision-Making Systems, Children's Privacy, Devices that Listen, Augmented Reality/Virtual Reality, Interfaces and Dark Patterns, and AdTech. The archived video and transcripts are posted on the event page.

Bringing Dark Patterns to Light: An FTC Workshop. In April 2021, the FTC hosted a virtual workshop exploring "dark patterns" – user interfaces that can have the effect, intentionally or unintentionally, of obscuring, subverting, or impairing consumer autonomy, decision-making, or choice. With over 1,500 unique viewers in attendance, panelists focused, in part, on how design elements obscure or subvert consumers' privacy choices. The archived video and transcripts are posted on the event page. Following on the workshop, the FTC issued a staff report, which discusses dark patterns in greater detail.

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 published, updated, or developed in 2021-2023 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. As the centerpiece of the FTC's outreach to small business on cybersecurity, the websites provide plain-language advice on how to protect computers and networks, but also how to train employees to keep data safe. FTC staff participated in dozens of events on cybersecurity in collaboration with federal partners, including the Small Business Administration (SBA), the National Institute of Standards and Technology (NIST), and the Cybersecurity and Infrastructure Security Agency (CISA). To expand outreach to every community, the FTC partnered with organizations that serve minority-owned businesses, such as the National Diversity Coalition and the Native Learning Center, as well as local business groups including the San Diego Hispanic Chamber of Commerce and the Dineh Chamber of Commerce, which represents Navajo business owners. FTC staff conducted webinars in Spanish to business owners in Rhode Island, Virginia, and Puerto Rico; and joined the National Cybersecurity Alliance, Identity Theft Resource Center (ITRC), cyber education associations, as well as state, local, and national government agencies in a Twitter chat to raise awareness about cybersecurity. To reach women small business owners, FTC staff conducted presentations at the New England Library Association's conference and at a regional SBA Women's Business Development Center.

  Business Guidance: The FTC published several new or updated business guidance documents designed to assist businesses in understanding their obligations to safeguard consumers' data and privacy—and what to do if something goes wrong. Focusing on health privacy, the FTC issued five new or revised publications: Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule, published in cooperation with HHS' Office for Civil Rights; Health Breach Notification Rule: The Basics For Business, a primer for companies new to the Rule; and Complying With the FTC's Health Breach Notification Rule, which answers FAQs that HBNR-covered organizations are asking. In addition, the FTC updated Mobile Health App Developers: FTC Best Practices, which offers tailored data security advice for app developers. Companies entering the health app business also can use the updated online Mobile Health App Interactive Tool – revised in cooperation with HHS and other agencies – to identify the federal privacy and security laws that may apply specifically to their products. Also new in 2022: FTC Safeguards Rule: What Your Business Needs to Know, a guide to help businesses understand the 2021 revisions to the Safeguards Rule.

  Consumer Guidance: The FTC updated its online privacy and security guidance at ftc.gov/onlinesecurity to give consumers the latest advice about understanding online privacy, protecting their devices from hackers and threats, and avoiding scams that try to steal their personal information. The FTC also updated a wide

variety of articles offering consumers current, actionable advice. Updated articles cover everyday issues, such as securing your internet-connected devices at home and removing personal information before you get rid of your computer or phone, and best privacy practices, such as using two-factor authentication to protect accounts and creating strong passwords. They also offer advice on serious problems consumers face, including dealing with stalking apps and avoiding and recovering from identity theft. For parents and kids, the FTC also recently updated its printed booklet and online article Heads Up: Stop. Think. Connect., which helps them understand and reduce the risks that come from socializing online.

- **Identity Theft Guidance:** After the height of the pandemic stimulus effort in 2021, the FTC worked closely with the SBA to help people whose personal information was used without their consent to apply for Paycheck Protection Program (PPP) loans or COVID-19 Economic Injury Disaster Loans (EIDL). Together, FTC and SBA staff identified and publicized a path for these individuals to report the identity theft and help clear any resulting damage to their credit reports. In addition, the FTC successfully broadened the scope and increased the reach of Identity Theft Awareness Week, the agency's annual identity theft campaign to help educate people about how to spot, avoid, and recover if it happens. FTC staff strengthened existing partnerships and forged new relationships with a variety of partners, including AARP, ITRC, Consumer Action), libraries, and federal agencies such as the Veterans Affairs Administration and Internal Revenue Service. Outreach efforts leveraged numerous webinars, podcasts, Facebook Live events, and Twitter (X) chats. In 2023, language enhancements to the FTC's Call Center and Consumer Sentinel Network expanded the agency's ability to serve more communities, particularly those who are more comfortable speaking in languages other than English. Now people can call to report identity theft and talk to someone in their own language to get steps to recover from identity theft. This also expands law enforcement's ability to see and act on scams affecting communities where they previously had limited access and visibility.

- **Business Alerts:** The FTC's Business Blog addressed and provided important context for recent enforcement actions, reports, and policy statements. The FTC published more than a hundred data security- and privacy-related Business Alerts on topics and cases ranging from SpyFone and CafePress to Twitter, Ring, and Amazon. Notable highlights include blogs providing a comprehensive summary of a series of FTC cases aimed at protecting the privacy of health information and blogs explaining FTC policy statements on education technology and the Children's Online Privacy Protection Act and the misuse of biometric data. Beginning in 2021, the FTC issued numerous business alerts on a range of

issues implicated by the emerging use and potential misuse of AI, as described above, including a comprehensive "AI and Your Business" blog series as well as posts addressing the importance of equity and fairness in AI and the application of bedrock privacy principles in data collecting.

- **Consumer Alerts:** The FTC's Consumer Blog regularly alerted readers to potential privacy and data security hazards and offered advice to help them protect their information. Relevant Consumer Alerts promoted a guide to protecting yourself online; offered advice on how to protect your connected devices and accounts and five things to do to protect yourself online; and warned people about scammy emails claiming their information was spotted on the dark web and ads for fake AI spreading malicious software. Alerts about FTC cases on data security and privacy also offered advice to consumers about using multifactor authentication and changing account passwords if their information is exposed in a data breach.

OFFICE OF TECHNOLOGY

The Commission continually develops its expertise in technology to help protect consumers in the 21st Century marketplace. In 2023, the Commission established the Office of Technology (OT) to assist the Commission by strengthening and supporting law enforcement investigations and actions; advising and engaging with FTC staff and the Commission on policy and research initiatives; and engaging with the public and relevant experts to understand trends and to advance the Commission's work.

Among other things, OT has taken a deep dive into the technical side of FTC's recent cases on digital health platforms, such as GoodRx and BetterHelp. It has explained the importance of effective breach disclosures, how interoperability can coexist with privacy and security, and how the FTC has worked to strengthen its remedies to address the underlying causes of risk in complex systems. In order to enhance security without compromising privacy, OT has emphasized that consumers should be able to rely on a company's promise that mobile numbers will be used for multifactor authentication, and not marketing.

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. Previously, in 2020, Congress renewed the U.S. SAFE WEB Act for another seven years.

The FTC participated in drafting the Global Cooperation Arrangement for Privacy Enforcement (Global CAPE), part of the effort to globalize the APEC Cross-Border Privacy Rules (CBPR) system. As a member of the Global Privacy Enforcement Network (GPEN) Committee, the FTC also hosted a workshop and led the development of a new Action Plan for GPEN.

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 2021-2023, the FTC played an important role in policy deliberations and projects on privacy and data security internationally. 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, the G7 Data Protection Authorities, and the Organisation for Economic Co-operation and Development, providing input on issues ranging from Artificial Intelligence 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, including with officials from Egypt, the United Kingdom, Canada, the European Data Protection Supervisor, the European Data Protection Board, and members of the European Parliament. Additionally, the FTC conducted several technical cooperation exchanges on privacy and cross-border data transfer issues, including with Kenya, the Philippines, and at several events on the Cross Border Privacy Rules system organized by the Department of Commerce.

Federal Trade Commission

ftc.gov