FTC Report on Resources Used and Needed for Protecting Consumer Privacy and Security

ThiFT7 (o)0.5 (u)0.5 (rc)1.7 (e)1.7 d.5 (ri)0.8 (ty)]x [66.01 .

- 147 cases alleging violations of Do Not Call, with orders totaling $1.7 billion in civil penalties, redress, or disgorgement, and actual collections exceeding $160 million
- 106 cases enforcing the Fair Debt Collection Practices Act, with more than $700 million ordered in monetary relief

In addition to our enforcement work, in the privacy and security area, we have hosted about 75 workshops and issued approximately 50 reports. Our Division of Consumer and Business Education has distributed more than 32 million print publications on privacy and security. We have received more than 48 million page views for business guidance and more than 28 million page views for our consumer education on this topic. As an example of our reach, our FAQ page on COPPA alone received more than 1.4 million page views. Several other units provide significant support for our enforcement and policy efforts, including the Office of International Affairs, the Office of Public Affairs, the Office of Policy Planning, and the Office of Congressional Relations.

Despite the relatively small number of employees dedicated to privacy enforcement, we have used our existing resources effectively, and we have brought more cases, and obtained larger fines, than any other privacy enforcement agency in the world. However, with additional resources, we could better ensure that American consumers' privacy is adequately protected. We currently have well under the number of Full Time Equivalent employees ("FTEs") that data protection authorities in other, much smaller, countries have. For example, the U.K. Information Commissioner's office has about 700 employees,[1] and the Irish Data Protection Commissioner has about 180 employees.[2] Although these entities have different mandates,[3] as the federal entity primarily

responsible for protecting consumers' privacy and data security in the United States, the FTC should have a more comparable number of employees or access to additional outside resources (such as experts).[4]

As laid out in Chairman Simons' letter to Representatives Pallone and Schakowsky, if the FTC were to obtain a sufficient amount of additional FTEs, we would consider adding at least three separate management units within the FTC with the following responsibilities:[5]

- De novo enforcement: One or more units would include resources from our existing privacy division, which would be expanded to do the following:
  - Investigate more websites, apps, and other online services for potential violations of the Children's Online Privacy Protection Act;
  - Additional investigations involving new technologies, such as Internet of Things, facial recognition, biometrics, and artificial intelligence, as well as stalking apps, revenge pornography, and other technologies that have the potential to result in substantial consumer harm;
  - Devote additional staff to enforcement involving the collection, use, and disclosure of sensitive data, including health data that falls outside of the Health Insurance Portability and Accountability Act and financial data covered under statutes we enforce such as the Gramm-Leach-Bliley Act and Fair Credit Reporting Act; and
  -

legislation would expand the agency's civil penalty authority, provide the agency with targeted rulemaking authority, and extend the agency's commercial sector ju (t)-sliis (M)d (al)1 pr (h

any company for violating consumers' privacy. The settlement is currently pending approval by the United States District Court for the District of Columbia.

In a related, but separate case, the FTC also filed a law enforcement action against the data analytics company Cambridge Analytica, as well as its former Chief Executive Officer, Alexander Nix, and app developer, Aleksandr Kogan. The FTC's complaint alleged that Cambridge Analytica, Nix, and Kogan used false and deceptive tactics to harvest personal information from millions of Facebook users for voter profiling and targeting. The complaint alleged that app users were falsely told the app would not collect users' names or other identifiable information. Contrary to this claim, the complaint alleged, the app collected users' Facebook User ID, which connects individuals to their Facebook profiles. Kogan and Nix agreed to settlements with the FTC that restrict how they conduct any business in the future, and the Commission entered a default judgment against Cambridge Analytica. The Commission's opinionCoCoCod the app woul brs[3

information from consumers. It is also required to notify consumers and delete the data unlawfully collected from consumers, unless it obtains their affirmative, express consent to maintain the e-receipts.

In Effen Ads, LLC (iCloudWorx), the FTC obtained stipulated final orders against defendants that promoted a work-from-home program through unsolicited email, or spam, claiming that consumers could make significant income with little effort. The spam emails included misleading "from" lines and links to websites that falsely claimed that various news sources had favorably reviewed the program, and "subject" lines that displayed false celebrity endorsements. The stipulated final orders permanently ban defendants from marketing or selling either work

unencrypted personal information—such as Social Security numbers and other sensitive data—of about 12.5 million consumers.

The FTC settled charges against InfoTrax Systems, a technology company that

Credit Reporting & Financial Privacy

The Fair Credit Reporting Act (FCRA) sets out requirements for companies that use data to determine creditworthiness, insurance eligibility, suitability for employment, and to screen tenants. The FTC has brought more than 100 cases against companies for violating the FCRA and has collected more than $40 million in civil penalties. The Gramm-Leach-Bliley (GLB) Act requires financial institutions to send customers initial and annual privacy notices and allow them to opt out of sharing their information with unaffiliated third parties. It also requires financial institutions to implement reasonable security policies and procedures. Since 2005, the FTC has brought about 35 cases alleging violations of the GLB Act and its implementing regulations. In 2019, the FTC brought the following cases:

The FTC has brought more than 100 cases against companies for violating the FCRA and has collected more than $40 million in civil penalties.

In the Equifax case, discussed above, the FTC alleged that the credit reporting agency violated the GLB Safeguards Rule. Specifically, the complaint alleged that Equifax failed to design and implement safeguards to address foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; regularly test or monitor the effectiveness of the safeguards; and evaluate and adjust its information security program in light of the results of testing and monitoring, and other relevant circumstances.

In Dealerbuilt, discussed above, the FTC alleged that the company violated the Safeguards Rule by failing to: develop, implement and maintain a written information security program; identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information; assess the sufficiency of any safeguards in place to control those risks; and design and implement basic safeguards and to regularly test or otherwise monitor the effectiveness of such safeguards' key controls, systems, and procedures.

International Enforcement

The FTC enforces the EU-U.S. Privacy Shield Framework, the Swiss-U.S. Privacy Shield Framework, and the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules System.

The EU-U.S. Privacy Shield Framework provides a legal mechanism for companies to transfer personal data from the European Union to the United States. This Framework, administered by the U.S. Department of Commerce, helps protect consumers' privacy and security through an agreed set of Privacy Shield Principles. The FTC plays a role in enforcing companies' privacy promises under the Framework as violations of Section 5 of the FTC Act. This year, the FTC participated, alongside the U.S. Department of Commerce and other U.S. government agencies, in the third Annual Review of the Framework, which became operational in August 2016. Following the review, the European Commission announced its continued support for the Privacy Shield, pointing to increased FTC enforcement actions as contributing to the effective functioning of the Framework.

The FTC also serves as a privacy enforcement authority in the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (AP(s)-1 (t)-3.1 (PTC)12rAP(s)-1 (t9e4)-2 (y)Syst (PTCe).14

During the past year, the FTC brought the following 13 cases:

In eight separate actions, the FTC charged that 214 Technologies, Click Labs, DCR Workforce, Incentive Services, LotaData, Medable, SecurTest, and Thru falsely claimed participation in Privacy Shield. While the companies initiated Privacy Shield applications with the U.S. Department of Commerce, the companies did not complete the steps necessary to be certified as complying with the Framework. Because they failed to complete certification, they were not certified participants in the Framework, despite representations to the contrary.

In separate actions, the FTC charged that Empiristat, Global Data Vault, and TDARX falsely claimed participation in Privacy Shield. The companies had allowed their certifications to lapse while still claiming participation. Further, the companies allegedly failed to verify annually that statements about their Privacy Shield practices were accurate, and failed to affirm that they would continue to apply Privacy Shield protections to personal information collected while participating in the program.

As a part of the FTC's action against Cambridge Analytica, described above, the FTC determined that the company falsely claimed to participate in Privacy Shield after allowing its certification to lapse. Among other things, the Final Order prohibits Cambridge Analytica from making misrepresentan the prng 62ca fmisr72k <</MCID 44

whether their actual data practices align with consumer expectations and public-facing statements.

The FTC testified before Congress numerous times on privacy and data security issues. For example, the Commission called for privacy and data security legislation in testimony before the House and Senate Appropriations Committees

RULES

Congress has authorized the FTC to issue rules that regulate specific areas of consumer privacy and security. Since 2000, the FTC has promulgated rules in a number of these areas:

The COPPA Rule requires websites and apps to get parental consent before collecting personal information from children under 13.

implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards. In 2019, the FTC issued a Notice of Proposed Rulemaking seeking comments on both the GLB Privacy and Safeguards Rules. The public comment period closed later in 2019,

free online credit monitoring for active duty military. In 2019, the FTC also participated in more than 40 identity theft-related outreach events, including: speaking at several national conferences on cybercrime and older adults; training Capital One attorneys at a Pro Bono Identity Theft Clinic; speaking at Credit Builders Alliance and World Elder Abuse Awareness Week events; and participating in numerous AARP webinars and tele-town halls. In addition, the agency worked with the Social Security Administration (SSA) to address Social Security imposters and set up IdentityTheft.gov/SSA to help people who get these scam calls. The FTC also worked with AARP to create three videos aimed at Asian American Pacific Islander older adults, helping them avoid IRS imposters, robocalls, and Medicare scams.

Consumer Blog. The FTC's Consumer Blog alerts readers to potential privacy and data security hazards and offers tips to help them protect their information. In 2019, the most-read consumer blog posts addressed how to avoid Social Security Administrat3 (i)24 Tm [(2019he 0 T.2 -0 0 2 (mi)4(i)1 (miu)-1 (m(2019he 0 T.20 Td [(C

Enforcement Cooperation

The FTC cooperates on enforcement matters with its foreign counterparts through informal consultations, memoranda of understanding, complaint sharing, and mechanisms developed pursuant to the U.S. SAFE WEB Act, which authorizes the FTC, in appropriate cases, to share information with foreign law enforcement authorities and to provide them with investigative assistance using the agency's statutory evidence-gathering powers. Significant enforcement cooperation developments in 2019 include:

Span <</MCID