ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy / Financial Services & Products
ADVISORY ■

AUGUST 23, 2022

CFPB and FTC Looking to Ramp Up Data Security Requirements

***By:** Kim Peretti, Brian Johnson, Kathleen Benway, Nanci Weissgold, and Lance Taubin*

On August 11, 2022, the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC) made waves by signaling their intent to crack down on inadequate data security controls to safeguard consumer personal information. The CFPB published a circular stating that "covered persons" or "service providers" (as defined in 12 U.S.C. 5481), including nonbank institutions and financial technology companies, may violate the Consumer Financial Protection Act (CFPA) for inadequate data security controls to safeguard sensitive consumer information. On the same day, the FTC issued an advance notice of proposed rulemaking (ANPR) to request public comment on whether new rules are needed to address the harms resulting from "commercial surveillance" and lax data security practices. Both the circular and the ANPR are broad and could establish extensive data security requirements for covered businesses that handle personal information.

The CFPB's Circular on Data Protection and Information Security

The CFPB asserts that failure to implement and maintain adequate security practices to protect sensitive personal information could constitute an unfair, deceptive, or abusive act or practice (UDAAP) in violation of the CFPA. A UDAAP is defined as an act or practice that (1) causes or is likely to cause substantial injury to consumers; (2) is not reasonably avoidable by consumers; and (3) is not outweighed by countervailing benefits to consumers or competition. The circular makes it clear that neither an "actual injury" nor a data breach or computer intrusion are required to run afoul of the CFPA's prohibition on a UDAAP—inadequate security measures alone may impose a significant risk to consumers and constitute a UDAAP.

Importantly, in the Dodd–Frank Act, Congress explicitly did not grant the CFPB the authority to write a Safeguards Rule or to enforce the Safeguards Rule. Indeed, the Safeguards Rule issued under the Gramm–Leach–Bliley Act (GLBA), which applies to the same financial institutions that fall under the CFPA and was promulgated by and is enforced by the FTC, not the CFPB, imposes certain affirmative obligations to maintain adequate security controls to protect consumers' personal information, including the requirement for nonbanking financial institutions to develop, implement, and maintain a comprehensive written information security program with appropriate administrative, technical, and physical safeguards. The recently amended FTC Safeguards Rule includes greater specificity on the necessary security controls. The circular asserts that the requirements in the Safeguards Rule and the prohibition on a UDAAP "often overlap, [but] they are not coextensive." Consequently, it appears that the CFPB, originally created by Congress in the Dodd–Frank Act, is using the existing legal structure to broadly interpret what security controls (or lack of security controls) would be considered a violation of the CFPA, despite the same statute denying the CFPB the authority to write or enforce a Safeguards Rule.

Through the circular, the CFBP does indeed appear to be venturing into data security regulation. While the CFPB explicitly "does not suggest that particular security practices are specifically required under the Consumer Financial Protection Act," it identifies the failure to implement three common data security practices—multi-factor authentication (MFA), adequate password management, and timely software updates—to potentially be inadequate data security. Certainly, since the CFPB has not generally provided other guidance on reasonable security or data security standards or practices, the question remains how it may otherwise interpret what would be considered adequate data security practices.

The FTC's ANPR on Commercial Surveillance and Lax Data Security Practices

The FTC issued the ANPR requesting public comment on whether new rules are necessary to protect consumers' privacy and information, specifically to curb "commercial surveillance" and strengthen companies' data security posture. The two Republican commissioners voted against issuing the ANPR, arguing that it is Congress that should enact comprehensive privacy legislation, not the FTC, and noted that because Congress is close to passing the American Data Privacy and Protection Act (ADPPA), issuing the ANPR is premature.

The ANPR covers an enormous array of data privacy and security topics, including: (1) harms to consumers from commercial surveillance; (2) unique harms to children; (3) cost-benefit analysis and considerations of a proposed rule; (4) artificial intelligence / machine learning and potential discrimination from such automated processes; (5) consumer consent, notice, transparency, and disclosure about commercial surveillance; and (6) remedies. The FTC provides a lengthy list of 95 questions (broken out by topic) on which interested parties can comment, including:

- Should, for example, new rules require businesses to implement administrative, technical, and physical data security measures, including encryption techniques, to protect against risks to the security, confidentiality, or integrity of covered data? If so, which measures? How granular should such measures be? Is there evidence of any impediments to implementing such measures?
- Do the data security requirements under COPPA or the GLBA Safeguards Rule offer any constructive guidance for a more general trade regulation rule on data security across sectors or in other specific sectors?
- Should the Commission take into account other laws at the state and federal level[s] (e.g., COPPA) that already include data security requirements. If so, how? Should the Commission take into account other governments' requirements as to data security (e.g., GDPR). If so, how?
- Which, if any, commercial incentives and business models lead to lax data security measures or harmful commercial surveillance practices? Are some commercial incentives and business models more likely to protect consumers than others? On which checks, if any, do companies rely to ensure that they do not cause harm to consumers?
- Are there practices or [security] measures to which children or teenagers are particularly vulnerable or susceptible?

Overall, it is evident the FTC wants to curb data collection, processing, and monetization practices and establish stricter, more prescriptive data security requirements as a means of incentivizing companies to make the proper investments in their privacy and data security programs.

Historically, the FTC has used its statutory authority under Section 5 of the FTC Act (which, similar to the CFPA, makes unfair or deceptive acts or practices in or affecting commerce unlawful) to bring enforcement actions against entities within its jurisdiction, including nonbank financial institutions and other companies that have insufficient data security controls to safeguard consumer personal information. The FTC has also promulgated rules pursuant to sector-specific statutes, such as the Children's Online Privacy Protection Act (COPPA) Rule and the recently amended Safeguards Rule.

According to the Democratic commissioners, these enforcement actions and sector-specific rules have resulted in a piecemeal regulatory approach to data privacy and security. This piecemeal approach, coupled with the (1) FTC's limited ability to seek monetary damages from first-time violators; (2) lack of adequate remedies (i.e., an injunction does not help a consumer whose personal information has already been compromised in a data breach); and (3) inability to obtain monetary relief for consumers who were not directly injured (which presumably would incentivize companies to implement strong data security controls across the board), has prompted the FTC to use its authority to approach data security by authoring rules under Section 18 of the FTC Act, more commonly known as Magnuson–Moss rulemaking.

Magnuson–Moss rulemaking requires the FTC to find "unfair or deceptive acts or practices" that are "prevalent." The finding can be based on FTC cease-and-desist orders or on "other information" indicating a "widespread pattern" of unfair or deceptive acts or practices. Since at least the 1980s, the FTC has generally declined to use its Magnuson–Moss rulemaking authority because of the extremely arduous process required to actually promulgate a rule using this authority—which on average has taken more than seven years. While FTC Chair Lina Khan acknowledged Magnuson–Moss's shortcomings, she noted it would allow the FTC to impose civil penalties on first-time violators (the FTC Act currently restricts the FTC in this regard). It appears that the FTC sees public comment in response to the ANPR as the "other information" that it may need to ultimately propose a new rule.

Perhaps, however, the lengthy rulemaking process will allow Congress the opportunity to consider the ADPPA; Commissioner Noah Phillips, in his dissent, raised concerns about derailing the ADPPA. The FTC is holding a public forum on September 8, 2022, with comments on the ANPR due October 21, 2022.

Key points in the ANPR include:

- Scope includes employees as well as consumers. The term "consumer" in the ANPR includes businesses and workers, not just individuals who transact with the business for goods and services. The FTC wants to protect not just traditional consumers, but companies' employees, which will likely require companies to reconsider their overall data privacy and security programs.
- Scope could apply broadly to a company's data privacy practices. The ANPR aims to enhance companies' data security practices and control "commercial surveillance." In the ANPR press release, the FTC defines "commercial surveillance" to mean "the business of collecting, analyzing, and profiting from information about people." This definition is broad, suggesting that the FTC's rules could dictate a company's entire data privacy practices. It appears that the FTC purposefully chose "surveillance" to express the breadth and pervasiveness of (problematic, in the FTC's eyes) data practices. Much of the data practices are unknown to consumers, which is a driving motivation in the ANPR: "Companies reportedly surveil consumers while they are connected to the internet—every aspect of their online activity, their family and friend networks, browsing and purchase histories, location and physical movements, and a wide range of other personal details."
- Prescriptive data security requirements may be considered. Given companies' general failure to implement reasonable security measures to protect personal information (in the FTC's eyes), the ANPR appears to suggest incorporating prescriptive data security requirements. The FTC defines "data security" broadly to mean "breach risk mitigation, data management and retention, data minimization, and breach notification and disclosure practices." The FTC may draw some of the prescriptive requirements from the recently amended Safeguards Rule implementing Section 501(B) of the GLBA, which includes detailed information security requirements that nonbanking financial institutions are required to implement as part of their information security programs. These prescriptive requirements include access controls, asset and data inventory, encryption of all customer information in transit and at rest (with some exceptions for compensating controls), secure development practices, MFA (with some exceptions for compensating controls), and periodic penetration testing and vulnerability assessments, among other security measures (some of which were effective on January 10, 2022,

and the rest coming into effect on December 9, 2022). Moreover, it will be interesting to see if a potential rule, under the "breach notification and disclosure practices" portion of the "data security" definition in the ANPR, incorporates the "de facto breach notification obligations," set forth in the FTC's recently published blog post, which uses Section 5 of the FTC Act to potentially create new breach notification obligations.

Even though the ultimate impact of the CFPB's circular and the FTC's potential final rule are unknown, it is clear that enhancing data security programs to protect personal information is a critical area companies cannot ignore. While no data security rule from the FTC is imminent, with the CFPB signaling that it intends to bring UDAAP enforcement actions against covered persons and service providers for failing to maintain adequate data security controls, covered persons and service providers should strongly consider reviewing their data security practices, especially for practices identified by the CFPB as potentially problematic (lack of MFA, inadequate password management, and untimely software updates), to protect systems that may access or store consumers' personal information.

You can subscribe to future ***Privacy, Cyber & Data Strategy*** and ***Financial Services & Products*** advisories and other Alston & Bird publications by completing our publications subscription form.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or the following:

Kimberly Kiefer Peretti
+1 202 239 3720
kimberly.peretti@alston.com

Brian Johnson
+1 202 239 3271
brian.johnson@alston.com

Kathleen Benway
+1 202 239 3034
kathleen.benway@alston.com

Nanci L. Weissgold
+1 202 239 3189
nanci.weissgold@alston.com

Lance Taubin
+1 212 905 9301
lance.taubin@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE: One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 4th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333