

## Cabinet News and Views

Informed analysis for the financial services industry



### CFPB and FTC Take Aim at Bevy of Data Practices



By [Mercedes Kelley Tunstall](#)  
Partner | Financial Regulation

In the heat of summer, the nation's top consumer protection agencies have issued startling and transformative statements and rules regarding data practice.

- First up, the Consumer Financial Protection Bureau [issued a so-called "interpretive rule"](#) (which means that no one was provided advance notice of the rule nor had the ability to challenge rule provisions) that concluded that digital marketing companies, particularly those that have major search engines on which companies can buy advertising, are "service providers" for purposes of the Consumer Financial Protection Act ("CFPA"). This rule means that such companies can, and presumably will, be held liable for violations of consumer financial services laws for advertisements that do not carry the proper disclosures or for marketing tactics that are deemed to be unfair, deceptive or abusive by the CFPB. Director Chopra noted in an accompanying speech that the "growing interest from Big Tech companies to find new ways to harvest and monetize our personal financial data" were behind the reason for the rule, referencing in particular a lawsuit HUD brought against Facebook alleging violations of the Fair Housing Act, because Facebook's systems help advertisers limit the audience for ads and target specific groups of people, to the exclusion of protected classes.
- Next, the CFPB [issued a circular](#) that reminded the consumer financial services industry about its obligations to protect data and ensure security for sensitive consumer information. The circular is written in a question-and-answer format and includes the CFPB's conclusion that failures to reasonably protect consumer information can and should constitute an unfair, deceptive or abusive act or practice under the CFPA. Largely referencing precedent from the Federal Trade Commission ("FTC"), the CFPB identified at least the following as basic elements for data protection (none of which are new): multi-factor authentication for customers to access their data; adequate password management internally (*i.e.*, requiring employees to change their

passwords regularly and to use strong passwords); and timely software updates to any programs that have access to or that process customer data.

- Finally, on August 11, the FTC issued an [advance notice of proposed rulemaking \(“ANPR”\)](#) regarding whether “new trade regulation rules or other regulatory alternatives concerning the ways in which companies (1) collect, aggregate, protect, use, analyze, and retain consumer data, as well as (2) transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive” are needed. The initial comment period for industry to address 95 separate areas of inquiry is sixty (60) days, and the FTC will hold a [public forum](#) on September 8 to discuss the ANPR.
-