Financial Services Management

Data-Safeguard Legal/Reputational Risk

Cite
CFPB, Consumer Financial Protection Circular 2022-04, Insufficient Data Protection or Security for Sensitive Consumer Information

Recommended Distribution:
IT, Compliance, Policy, Legal, Government Relations

Website:
https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/

Impact Assessment

- The CFPB has now taken on prudential responsibilities with regard to data-system operations and resilience by virtue of standards that must be met in an arena once seen solely as the province of safety-and-soundness regulators or the FTC.
- The agency may find a UDAAP violation if it deems there to be insufficient data safeguards even in the absence of actual injury to any consumer, sharply increasing legal and reputational risk in this area and in any others where the rationale presented here for liability may be deemed by the Bureau to apply.
- Third-party IT service providers are subject to these CFPB standards, increasing both the demands consumer-finance companies will make of them and their legal/reputational risk.

Overview

Using another of its tools to set policy without prior public comment, the CFPB has released a circular stating that inadequate consumer-data safeguards may constitute a breach of the unfair, deceptive, or abusive acts or practices (UDAAP) protection standards subject to Bureau enforcement action. This is the case even if no consumers have been harmed, if only one consumer is adversely affected, or if a small amount of actual or potential damage puts many consumers at risk. The Bureau also prescribes data-safeguard standards firms and service providers must ensure to comply with CFPB expectations.

Impact

This circular expands the CFPB's interpretations of law regarding UDAAP, its authority over nonbanks such as fintechs and bigtech, and its broad reading of "service providers" also subject to its rules on data-security issues many firms likely think are now principally business matters related to risk tolerances and market expectations. The circular references a 2021 FTC rule mandating data safeguards akin in some ways to those governing banks under the Gramm-Leach-Bliley Act and other statutes, regarding these as essential elements which, as discussed in more detail below, are essential to preventing the kind of consumer harm the Bureau believes to constitute UDAAP. CFPB Director Chopra was an FTC commissioner at the time this rule was enacted and thus may well view it as a vital protection; in the release accompanying this rule, he specifically cited credit-reporting agency lapses as one justification for this strong new CFPB policy. The circular's rationale is also based in part on one case pertaining to Equifax even though the Bureau in this instance found only "unfairness," not also UDAAP. Several FTC cases and litigation involving nonbanks are also used to demonstrate consumer harm related to data safeguard failings. A proposal from the FTC on new data safeguards the same day the CFPB issued its release may well have also influenced Mr. Chopra's thinking.

Under this circular, even a small data-security glitch could lead to significant legal and reputational risk if a large group of consumers is even slightly inconvenienced or if the source of the system failure is external to the financial company or its service provider. As a result, even a short-term outage in web access or that to the payment system could be deemed UDAAP, a finding more likely if the Bureau also does not believe consumers were appropriately remunerated and/or systems quickly remediated.

The harm the Bureau would need to find appears linked solely to lapses related to "sensitive" personal information, but what constitutes this information or if other failures might also lead to UDAAP penalties is not made clear. Rules in this area typically govern "personally-identifiable information" such as names and addresses, but the Bureau's choice of wording suggests it may apply also to the behavioral data or other information recently targeted in an interpretive ruling related to digital marketing.

The CFPB's circular also states that UDAAP may exist even in the absence of actual injury to any consumer if safeguards are found to be weak. It appears thus to be taking on the supervisory role long presumed to reside principally with bank regulators with regard to safety and soundness and, to the extent FTC rules apply, to many nonbanks. The FTC does not have the broad enforcement power the Bureau claims and bank regulators tend in the absence of severe failings or findings of gross negligence to issue nonpublic supervisory orders when they believe systems standards do not suffice. The Bureau's policy may create jurisdictional conflicts, allow for more costly enforcement actions than the FTC or banking agencies on their own might contemplate, and otherwise increase legal and reputational risk in this arena. Consumers would, however, likely benefit from heightened resilience and more compensation in the event of data-safeguards incidents.

What's Next

This circular was issued on August 11 and is effective upon issuance. As with other CFPB rulings, entities targeted for enforcement actions may counter that the Bureau here acted without first following appropriate administrative procedure. The sweeping nature of this edict may also raise jurisdictional uncertainties. However, unless or until the Bureau is overruled in the courts or by Congress, its policies stand and covered entities and their service providers are at legal and reputational risk in the event the agency determines there to be any data-safeguard weakness.

Analysis

A. Scope

As noted, this circular states that the Bureau's belief that covered persons – i.e., banks and nonbank consumer-finance companies – and their service providers are covered by the Bureau's interpretation of UDAAP and now applied to data safeguards. The agency does so on grounds that UDAAP may occur with any action that causes or is likely to cause "substantial injury" to a single consumer or small injury to many consumers that is not "reasonably avoidable" by the consumer or outweighed by countervailing benefits to consumers or competition. How the Bureau would determine that markets are suitably competitive and thus that harm has not occurred is not made clear.

The circular goes on to say that practices such as "inadequate" authentication, poor password management, or insufficient software updating are likely to cause such injury without countervailing benefit. A breach or intrusion is not required for a demonstration of substantial harm.

B. Rationale

This circular is premised on the view that consumers have no way to judge data safeguards at consumer-finance providers, let alone those of the company's service providers. The Bureau also goes into detail on essential data safeguards where lapses or insufficiencies are likely to lead to substantial consumer harm without countervailing benefit.

Federal Financial Analytics, Inc.
2101 L Street, N.W., Suite 300, Washington, D.C. 20037
Phone: (202) 589-0880
E-mail: info@fedfin.com Website: www.fedfin.com