Cooley

August 19, 2022

On August 11, 2022, the Consumer Financial Protection Bureau published a Consumer Financial Protection Circular taking the position that providing "[i]nadequate security for the sensitive consumer information collected, processed, maintained, or stored by … [a] company can constitute an unfair practice" under the Consumer Financial Protection Act (CFPA).[1] Because insufficient data security is likely to cause substantial injury to consumers that is not reasonably avoidable or outweighed by countervailing benefits to consumers or competition,[2] the CFPB considers this to be an unfair practice – even in the absence of a data breach.

CFPB asserts expanded authority for information security

Financial institutions that provide services to consumers are subject to the requirements of the Gramm-Leach-Bliley Act (GLBA). The GLBA requires covered financial institutions and service providers to maintain an information security program with several specific requirements, such as imposing limitations on who can access customer information, requiring the use of encryption to secure information, and requiring the designation of a single qualified individual to oversee an institution's information security program (the Safeguards Rule). The GLBA's Safeguards Rule is implemented by the Federal Trade Commission (FTC).[3] In the August 11 circular, the CFPB asserts that information security programs are also subject to CFPB oversight, as maintaining adequate consumer data protections would be required to comply with the CFPA's prohibition on unfair, deceptive, or abusive acts or practices (UDAAP). An unfair act or practice is one that:

1. Causes or is likely to cause substantial injury to consumers.
2. Is not reasonably avoidable by consumers.
3. Is not outweighed by countervailing benefits to consumers or competition.[4]

The CFPB enumerates several instances where inadequate data security practices are likely to cause substantial injury to consumers, including through data breaches, cyberattacks, exploits, ransomware attacks and other exposure of consumer data.[5] Such harms are not reasonably avoidable to consumers, as information security programs are controlled or implemented by the financial institution, and the consumer has little say over these programs. The CFPB also notes that in conducting the balancing test required by the third UDAAP prong, it "expects" that the risk of substantial injury to consumers will outweigh any benefits to consumers or competition through cost savings.

Further, the CFPB attempts to support its conclusion through a review of caselaw that identified instances in which data management practices were evaluated in reference to the FTC's prohibition on unfair acts or practices. For example, in 2006, the FTC sued an online check processor alleging that it was an unfair practice to create and deliver checks without properly verifying that the person requesting the check was authorized to draw on the associated bank account.[6] The court concluded that failing to conduct adequate identity verification indeed violated the FTC Act's UDAAP provision. In 2012, the FTC sued several associated entities for failing to use appropriate measures to protect personal information from unauthorized access.[7] In that case, a court confirmed that the FTC had the authority under the FTC Act to regulate cybersecurity as a potentially unfair act.

The CFPB also outlined actionable steps financial institutions can take to protect consumer data, including:

1. Implementing multi-factor authentication.
2. Creating password management policies and procedures.
3. Providing timely software updates.

Renewed focus on data privacy?

In 2016, the CFPB issued a consent order against a payment processor alleging that the company had engaged

in deceptive acts and practices in violation of the CFPA relating to false representations made regarding the company's data security practices. In that instance, the CFPB's decision to issue the consent order was connected in large part to the fact that the company had represented to consumers that the company employed "reasonable and appropriate" measures to protect consumer data from unauthorized access. But the consent order identified several elements of the company's data security program that belied this representation, including that the company failed to:

1. Use appropriate measures to identify reasonably foreseeable security risks.
2. Provide adequate employee training.
3. Use encryption technologies.

In many ways, the recent circular revives UDAAP as a tool previously used by the CFPB to require enhanced consumer protections related to the offering and provision of financial services. That said, the 2016 consent order focused on affirmative representations the company had made to consumers. The August 11 circular thus goes further in arguing that a lack of adequate data security measures can constitute a UDAAP violation independent of any representations made by a covered entity.

Jurisdictional questions

The circular also creates several jurisdictional questions regarding oversight of the data security practices of consumer financial institutions. As acknowledged in the circular, the CFPB believes that a covered entity's insufficient data protection or information security practices could both trigger UDAAP liability under the CFPA **and** violate the GLBA Safeguards Rule. Conversely, it is less clear whether there are instances in which information security practices could be considered an unfair act or practice, but not a violation of the Safeguards Rule (or vice versa).

It also appears that the CFPB and FTC could be taking a collaborative approach to the protection of consumer data held by financial institutions. On the same day that the CFPB issued its circular, the FTC announced an advance notice of proposed rulemaking (ANPR) seeking public comment on commercial surveillance practices. While the ANPR did not specifically address the role of financial institutions in consumer data collection, it is clear that financial institutions that collect, store and transmit sensitive consumer data should take steps to ensure proper data integrity and security policies and procedures are in place, as these issues appear to be key initiatives for both agencies.

Notes

1. 12 US Code § 5536(a)(1)(B).
2. 12 USC § 5531.
3. The GLBA also includes privacy protections that require financial institutions to provide customers with initial and annual privacy notices, and limit the circumstances under which a financial institution may disclose nonpublic personal information about a customer or consumer. The Privacy Rule is implemented by the CFPB through Regulation P.
4. *Id.*
5. Actual injury is not required to satisfy this prong.
6. *FTC v. Neovi, Inc.*, 598 F. Supp. 2d 1104 (S.D. Cal. 2008) (No. 06 Civ. 1952), aff'd, 604 F.3d 1150 (9th Cir. 2010).
7. *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014) (No. 13 Civ. 1887), aff'd, 799 F.3d 236 (3d Cir. 2015).

Key Contacts

Adam Fleisher Washington, DC	afleisher@cooley.com +1 202 776 2027
Obrea Poindexter Washington, DC	opoindexter@cooley.com +1 202 776 2997