BLACK | MANN & GRAHAM L.L.P.

Attorneys At Law

17824 Mound Road, Suite C

Cypress, TX 77433

Phone: 713-871-0005

Fax: 713-871-1358

August 16, 2022

To: Clients and Friends

From: David F. Dulock

Subject: Consumer Financial Protection Circular 2022-04: Insufficient data protection or security for sensitive consumer information

On August 11, 2022, the CFPB issued the above Circular 2022-04 (herein "Circular") in which the CFPB answers the question "Can entities violate the prohibition on unfair acts or practices in the Consumer Financial Protection Act (CFPA) when they have insufficient data protection or information security?"

The Circular answers "Yes" to that question. It states: "'[C]overed persons' and 'service providers' must comply with the prohibition on unfair acts or practices in the CFPA. Inadequate security for the sensitive consumer information collected, processed, maintained, or stored by the company can constitute an unfair practice in violation of 12 U.S.C. 5536(a)(1)(B)." "Covered person" is defined in 12 U.S.C. 5481(6) as "(A) any person that engages in offering or providing a consumer financial product or service; and (B) any affiliate of a person described in subparagraph (A) if such affiliate acts as a service provider to such person." "Service provider" is defined in 12 U.S.C. 5481(26) as "any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service."

The Circular uses the specific criteria in the FTC's Safeguards Rule (Section 501(b) of Gramm-Leach-Bliley Act), which "limit who can access customer information, require the use of encryption to secure such information, and require the designation of a single qualified individual to oversee an institution's information security program and report at least annually to the institution's board of directors or equivalent governing body," in stating "[i]n certain circumstances failure to comply with these specific requirements may also violate the CFPA's prohibition on unfair acts or practices." An unfair act or practice is defined in 12 U.S.C 5531(c) of the CFPA as an act or practice "(1) that causes or is likely to cause substantial injury to consumers, (2) which is not reasonably avoidable by consumers, and (3) is not outweighed by countervailing benefits to consumers or competition."

In the Circular, CFPB explains one way an unfair act or practice, as defined in the CFPA, causes substantial injury to consumers is "when it causes significant harm to a few consumers or a small amount of harm to many consumers." The CFPB further explains that actual injury is not always required for an unfair act or practice to cause substantial injury to a consumer under the CFPA; "[a] significant risk of harm is also sufficient." For example, "inadequate data security measures that have not yet resulted in a breach" is an unfair practice that "is likely to cause substantial injury to consumers."

The Circular states "[w]hile the prohibition on unfair practices is fact-specific, the experience of the agencies suggests that failure to implement common data security practices will significantly increase the likelihood that a firm may be violating the prohibition." The Circular identifies the three measures below "as reasonable cost-efficient measures to protect consumer data[.]"

However, as written in the Circular, these measures describe a covered person or service provider not implementing these measures so that "the Circular describes conduct that will typically meet the first two elements of an unfairness claim . . . and thus increase the likelihood that an entity's conduct triggers liability under the CFPA's prohibition of unfair practices."

These measures have been edited in this memorandum to point out that implementing these measures are reasonable ways to protect consumer data.

1. Multi-factor authentication: Multi-factor authentication (MFA) is a security enhancement that requires multiple credentials (factors) before an account can be accessed. A common MFA setup is supplying both a password and a temporary numeric code to log in. Another MFA factor is the use of hardware identification devices. MFA solutions that protect against credential phishing, such as those using the Web Authentication standard supported by web browsers, or a reasonably secure equivalent to an MFA, are especially important.

2. Password Management: Includes adequate password management policies and practices, including processes in place to monitor for breaches at other entities where employees may be re-using logins and passwords (including notifying users when a password reset is required as a result) and includes use of default enterprise logins or passwords.

3. Timely Software Updates: Routinely update systems, software, and code (including those utilized by contractors) and update them when notified of a critical vulnerability. This includes having asset inventories of which systems contain dependencies on certain software to make sure software is up to date and highlight needs for patches and updates. It also includes not using versions of software that are no longer actively maintained by their vendors.

Recipients of this memorandum should read Circular 2022-04 and not rely exclusively on this summary to comply with the Circular.