Fintechs Beware: CFPB Builds on FTC Safeguards for Consumer Data

August 19, 2022

On August 11, 2022, the Consumer Finance Protection Board issued Consumer Financial Protection Circular 2022-04 for enforcers of federal consumer financial laws. The new Circular reflects the consumer watchdog's increasing focus on the data security measures required for consumer data. The guidance targets financial companies and financial technology providers ("fintechs") for lack of such measures, deeming such failures a potential "unfair practice" under the Consumer Financial Protection Act.

"Financial firms that cut corners on data security put their customers at risk of identity theft, fraud, and abuse," said CFPB Director Rohit Chopra, in a statement. "While many nonbank companies and financial technology providers have not been subject to careful oversight over their data security, they risk legal liability when they fail to take commonsense steps to protect personal financial data."

To constitute an unfair practice under the CFPA, an act or failure to act must be likely to cause substantial injury that a consumer cannot reasonably avoid (absent countervailing benefits to consumers or competition). In this most recent guidance, the CFPB does not mandate specific data security measures, but it indicates that a financial company's failure to implement certain basic measures will not be justifiable.

According to the CFPB, what are the minimum basic measures that your fintech or financial company should have in place now?

- *Multi-factor Authentication*: Multi-factor authentication (MFA) requires multiple credentials before an account can be accessed.[1] MFA makes it harder for threat actors to compromise user and employee accounts and access sensitive data.
- *Adequate Password Management*: Your company should impose complexity and expiration requirements for passwords. Without them, it may be hard for you to convince the CFPB or other enforcement entity (e.g., the FTC or a state attorney general's office) that an unfair practice does not exist.[2]
- *Timely Software Updates*: Enforce "Patch Tuesday" or similar initiatives, and perform updates to software, including open source software, as soon as possible. Failure to do so can leave your system open to a known security vulnerability.

Fintechs have historically avoided the regulatory spotlight. Given the recent growth in their numbers and types of financial services, however, the CFPB is increasing its enforcement efforts over this sector,

particularly at a time of agency concerns over Big Tech's entry into the banking and consumer payment service markets. At this same time, the FTC is focused on data security under its Safeguards Rule.

The area of data security and privacy is constantly changing and is only growing in importance and presenting additional risk to many organizations. Lathrop GPM LLP can assist your organization in understanding its data security and privacy obligations.

[1] *See Back to Basics: What's multi-factor authentication - and why should I care?*, National Institute of Standards and Technology, https://www.nist.gov/blogs/cybersecurity-insights/back-basics-whats-multi-factor-authentication-and-why-should-i-care .

[2] *See Good Security Habits*, CISA, (Feb. 1, 2021) Good Security Habits | CISA .