Federal Trade Commission Updates Cybersecurity “Safeguards Rule” for Financial Institutions

Article By

Caitlin Throne
Kurt R. Hunt
Christian Gonzalez

Dinsmore & Shohl LLP
Publications

Monday, November 1, 2021

Last week, in the culmination of a process that began in 2016, the Federal Trade Commission (FTC) issued a Final Rule to update the Safeguards Rule promulgated under the Gramm-Leach-Bliley Act. The Safeguards Rule applies to financial institutions, including non-banking companies “significantly engaged” in providing financial products or services such as mortgage brokers, automotive dealers, and payday lenders, requiring those institutions to develop and implement comprehensive security to keep their customers’ information safe.

Cyberattacks and other threats to consumer data have increased over the course of the COVID-19 pandemic, escalating regulatory scrutiny and business risks. These
new changes to the Safeguards Rule largely focus on clarifying expectations for financial institutions, including:

- **More detailed requirements.** The Final Rule creates clearer expectations with more detailed requirements for how financial institutions should develop and establish their information security programs, such as setting clearer requirements for employee training, establishing that risk assessments must be set forth in writing, and increasing safeguards through data encryption and authentication.

- **Qualified Individual.** In order to increase accountability, the Final Rule designates one key person (to be known as the Qualified Individual) at each financial institution to be responsible for overseeing and enforcing the information security program.

- **Board reporting.** Financial institutions must schedule periodic reports on the information security programs to their board of directors or governing bodies, in hopes that the programs will receive the support and resources necessary for successful maintenance.

- **Change in scope.** The Final Rule expands the definition of financial institutions to include “finders”—companies that bring together the buyers and sellers of a good or service, in a move that makes the definition of financial institution more analogous to that in the Bank Company Holding Act. In addition, some financial institutions that collect information on fewer than 5,000 consumers are exempted from written risk assessment, incident response plan, and board reporting requirements.

Financial institutions regulated by the GLBA should familiarize themselves with the updated Safeguards Rule and evaluate their information security policies, focusing on ensuring they are compliant with the new requirements. The FTC also announced it is soliciting comments regarding reporting of data security incidents, signaling the possibility of additional changes in the near future.

© 2021 Dinsmore & Shohl LLP. All rights reserved.

National Law Review, Volume XI, Number 305