Proposed Rulemaking: Amendments to Safeguards Rule (16 CFR Part 314)

COMMENT LETTER

Proposed Rulemaking: Amendments to Safeguards Rule (16 CFR Part 314)

July 31, 2019
|
Download PDF

Access the Full Letter [PDF]

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, DC 20580

Dear Sir or Madame:

The Conference of State Bank Supervisors ("CSBS") appreciates the opportunity to comment on the Federal Trade Commission's ("FTC" or "Commission") notice of proposed rulemaking to amend its Safeguards Rule (RIN 3084-AB35). Whereas the existing rule laid out general elements of required information security systems, the proposed amendments contain specific requirements that address multiple aspects of a covered institutions information security system. State regulators believe the addition of specific safeguard requirements will provide covered financial institutions with needed clarity and guidance regarding how to structure and maintain effective information security programs. We have written this letter to address the question of how the proposed amendments relate to state law.

CSBS is the nationwide organization of banking regulators from all 50 states, American Samoa, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands. State regulators charter and supervise 79 percent of all banks in the United States. In addition, state regulators are the primary licensing authority and supervisor for a variety of non-depository industries covered by the FTC's Safeguards Rule, including mortgage lenders and servicers, payday lenders, money service businesses, non-federally insured credit unions, among others. CSBS, on behalf of state regulators, operates the Nationwide Multistate Licensing System (NMLS) as the database of record for the licensing and registration of more than 24,000 entities that provide nonbank financial services across multiple industries.

The Safeguards Rule was promulgated following the enactment of the Gramm-Leach-Bliley Act (GLBA) and since 2003 has required certain nonbank financial institutions to protect the financial information of their customers. The proposed amendments, modeled in-part on cyber-security regulations issued by the New York Department of Financial Services (NY DFS) and the insurance data security model law issued by the National Association of Insurance Commissioners in 2017, would add specific requirements to the general expectations

regarding safeguards requirements imposed on covered nonbank financial institutions.

While the enactment of GLBA in 1999 was an important development for financial institution information security, many states already had laws in place requiring financial institutions to take steps to safeguard consumer information. Importantly, GLBA expressly preserved the right of states to enact and enforce state laws that were more protective of consumers by ensuring the Act and its implementing regulations serve as a floor for data breach and data security protections.[1] This framework has allowed for states to be flexible and responsive in calibrating regulatory requirements as the rapid proliferation of online financial services has changed the way financial institutions interact with consumers and their financial data. Indeed, the FTC's decision to model the proposed amendments on the NY DFS cyber- security regulation is an implicit acknowledgement of the leadership role played by states in setting data security standards.

The proposed rule requests comments on the extent to which the proposal would preempt state laws. In addressing this question, it is important to consider the language of Section 507 and the approach previously taken by the FTC in making preemption determinations under Section 507. As codified, Section 507 states:

"(a) In general. This subchapter and the amendments made by this subchapter shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order or interpretation is inconsistent with the provisions of this subchapter and then only to the extent of the inconsistency.
(b) Greater protection under State law. For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subchapter if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter and the amendments made by this subchapter . . .". 15 U.S.C. § 6807.

Following the enactment of GLBA, several states submitted petitions to the FTC requesting a determination whether their laws were preempted under this provision.[2] In response to these petitions, the FTC determined that the individual state laws were not preempted by GLBA.[3] In making these determinations, the FTC conducted a two-step analysis to, first, determine whether the state law is "inconsistent" with federal law, and, second, to determine whether the state law affords "greater protection" than that provided by GLBA.

To determine whether a state law is inconsistent with the federal law, the FTC applied a two-part test to assess whether (1) compliance with both the state and federal laws is physically impossible or (2) the state law frustrates or thwarts the purpose of the federal statute. Importantly, the FTC determined that if the state law is not found inconsistent under either standard, then there is no need to determine whether the state law affords greater protection because Section 507 will not preempt state law absent a finding of inconsistency. In making these preemption determinations, the FTC noted that it would be very rare for a state law to be preempted under this two-part test. As the FTC considers future requests for preemption determinations, we encourage it do so on a case-by-case basis and in reliance on the precedent set by former determinations.

Provisions within certain state regulations will differ from those in the FTC's proposed Rule. For example, state laws may require covered entities to notify their state regulator of cybersecurity events within a set period. The FTC's proposed amended Safeguards Rule does not contain any such notification requirement. State regulators do not see a conflict in these requirements that would prevent an entity complying with the proposed rule from also satisfying a state notification requirement. In these cases, a state notification requirement would afford greater protections than the federal rule, but an assessment of that point is not necessary given that compliance with both the state and federal law are possible. We appreciate the inclusion of language in the proposed rule's commentary noting that requirements within the rule (such as the required creation of an incident response plan) are not intended to conflict with any independent reporting or notification requirements to which financial institutions are already subject.

Also, the commentary notes that a federal breach notification standard under GLB would be largely redundant because of state breach notification laws.[4]
Some argue that Congress should determine whether to preempt state laws in the data privacy and security space. State regulators strongly oppose any federal proposal which seeks to preempt states from playing a leading role in advancing consumer protections in the areas of data privacy, security, and control. In March, CSBS provided comments outlining our concerns regarding preemption in response to the Senate Banking Committee's request for feedback on data security and data privacy issues[5].

In recent years, there have been many examples of states taking a leadership role by enacting state laws that enhance consumer protections in the areas of data privacy, security and control. In addition to the regulations promulgated by the New York Department of Financial Services, over the past two years, New Jersey enacted a law that limits a merchant's ability to collect information about shoppers and pass that data onto third parties, Vermont enacted a law regulating data brokers, and Colorado and California enacted comprehensive data security standards. State regulators have also been active in responding to incidents that reveal weaknesses in data security practices by existing companies. State regulators were the only regulators that examined and took action against Equifax following the large-scale data breach in 2018. Following a joint examination by eight states, the states entered into a consent order with the company to address serious deficiencies in the company's cybersecurity program that resulted in the breach. The proximity of states to their consumers, and their proven ability to respond when necessary demonstrates the importance of preserving the concurrent enforcement framework in which federal law is a floor and states can enforce stricter requirements for data security and privacy.

State regulators believe this framework has been effective in protecting consumers. The proposed amendments to the Safeguards Rule would bolster the consumer protections ensured by the rule and would not prevent states from imposing stricter requirements. State regulators look forward to continued engagement with the FTC on this important topic.

Sincerely,

John Ryan
President and CEO

---

1 15 U.S.C. § 6807

2 See June 7, 2002 Letter from FTC Office of the Secretary to CT Banking Commissioner, available here.

3 See Benoit and Lovoy, "Update on Consumer Financial Privacy Legislation and Regulation", The Business Lawyer, Volume 58, No. 3, 1171-1176 (May 2003).

4 See footnote 123 in NPR

5 CSBS Comments on Legislative Efforts on Data Privacy and Security. March 14th, 2019. Available here: https://www.csbs.org/csbs-comments-legislative-efforts-data-privacy-and-security

Related Topics
Cybersecurity

Related Posts