Data Privacy & Data Security

Data privacy and data security are two distinct yet interconnected issues. With the rise of “big data” and its various uses, there has been a significant uptick in interest surrounding consumer expectations and the responsibilities of financial institutions. While states have been engaging with these issues in various ways, federal action is on the horizon. These issues naturally cross state borders, and it is imperative that any further action on data privacy and data security be done at the federal level, removing any confusion that might be caused by the varying state level requirements.

OVERVIEW

- Federal laws on consumer privacy and data security cover various industries and individuals, but there is no federal data breach notification law.
- Privacy and data security for financial institutions is governed by the Gramm-Leach-Bliley Act (GLBA). Under the GLBA are two regulations, Regulation P (data privacy) and the Safeguards Rule (data security).
  - The Bureau of Consumer Financial Protection (CFPB) has authority over Regulation P, which governs the treatment of non-public personal information about consumers.
  - The Federal Trade Commission (FTC) has authority over the Safeguards Rule, which sets forth standards for reasonable data security safeguards to protect customer information.
- States have recently taken on the issues of data privacy and data security. Additionally, every state has its own data breach notification law, each with their own varying requirements. Some key developments are:
  - Last year, California enacted the California Consumer Privacy Act (CCPA). This sweeping bill with extensive data privacy requirements is set to take effect on January 1, 2020, subject to several possible amendments.
  - Many states have begun introducing bills mirroring the CCPA, some with variations.
  - Importantly, some of these bills, like the CCPA, contain an exemption for data subject to the GLBA. Unfortunately, other bills require confusing conflict analysis to determine whether a federal or state requirement is applicable.
- The GLBA does not provide a private right of action, but states are considering broad private rights of action that punish businesses who are victimized by bad actors who actively evade security measures to steal their data.

For more information, visit mba.org or call (202) 557-2700.
IMPACT

- There are industry-specific efforts on data security, but there is no widespread standard for breach notifications.
  - With every state having its own breach notification statute, companies are subject to significant variations.
  - States are pursuing additional changes to their breach notification statutes, further complicating the regulatory environment.
  - A federal, preemptive, data breach notification would provide significant relief to businesses and clarity for consumers.
- Federal regulators have approached data security with significant care, allowing companies flexibility and encouraging adaptability in the face of a rapidly changing technological environment. State efforts to address data protection have the potential to create conflicts and confusion that only heighten the risk to businesses and consumers.
- Privacy legislation introduced by the states has high potential for variation that can lead to conflicting regulatory regimes.
  - Some of these proposed bills have been compared to the European Union’s General Data Protection Regulation (GDPR) for its overarching approach and significant impact on business.
  - Several questions remain with how these potential laws interact with the GLBA, how state regulators will interpret new definitions of personal information, and which entities are ultimately impacted.
  - A federal data privacy law would provide much needed clarity with a regulator in place to address specifics and set clear rules of the road for all market participants.

MBA’S POSITION / NEXT STEPS

- MBA has generally advocated for federal legislation on matters of data privacy and data security. In letters to the Treasury, CFPB, and Congress, MBA has expressed a need for uniformity in light of the national nature of operations involving data and the Internet.
- Currently, the FTC is soliciting comments on proposed changes to its data security requirements. Any efforts on the part of Congress to address protecting consumer information should take note of the industry response to the FTC’s proposed rulemaking.
- With the many nuances of data privacy and data security, and its interconnected nature to various industries, Congress should generally avoid prescriptive legislation and allow the appropriate federal regulators to seek uniformity in addressing these highly technical issues with stakeholder input.