sifma

Invested in America

November 8, 2019

The Honorable Phil Mendelson
Chair, Council of the District of Columbia
Chair, Committee of the Whole
Wilson Building, Room 412
1350 Pennsylvania Avenue, N.W.
Washington, DC 20004

RE: DC B23-215, A Bill Regarding Data Privacy Protection

Dear Chair Mendelson:

The Securities Industry and Financial Markets Association[1] is a national trade association which brings together the shared interests of over 340 broker-dealers, banks and asset managers, many of whom have a strong presence in the District of Columbia. We thank you for the opportunity to provide feedback on B23-215, which would generally modernize the District's data breach law while keeping the law in line with similar requirements across the country.

SIFMA generally supports such efforts and commends Attorney General Racine and the Council on their efforts in this space. Below we have included several suggestions for your review that would both strengthen consumer protections and increase the proposed framework's efficiency:

- **<u>The Need to Expand the Gramm-Leach-Bliley Act Compliance Provision</u>**

  The current law states that entities subject to Title V of the GLBA, and who provide notice of a breach in accordance with that Act, are deemed to be compliant with the District's law. As currently drafted, B23-215 would add two new provisions to the existing law, both of which would be outside of the GLBA deemed-compliance provision: notification to the District Attorney General, and an additional security requirement. We urge you to consider expanding the GLBA deemed-compliance provision to include both provisions, or at least modifying the notification provision, for the reasons discussed below.

  Public Records Requests

  The proposed AG notification provision includes requirements that the cause or nature of the breach and the identity of the responsible individual be reported. Our membership has expressed significant concern that this information could be made public through a public records request, which could cause significant additional security issues. Generally, disclosing the nature or cause of a breach could reasonably lead to the inadvertent disclosure of critical system and/or security information – which

[1] SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's nearly 1 million employees, we advocate for legislation, regulation and business policy, affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. For more information, visit http://www.sifma.org.

would only be made worse if that information could also be made public. Such a disclosure could put the personal information of people in D.C. and across the country at greater risk. Similarly, reporting the name of the individual who is responsible for a breach, if known, is problematic because it could be difficult to identify a single responsible person. Additionally, the need to identify a person(s) responsible may impact an organization's decision as to how – or even if – to report, which would defeat the intent of the proposal. Should you choose not to expand the GLBA deemed-compliance provision to the AG notification, we urge you to either remove these requirements (in subsections 3 and 6), or at least ensure that such reports are exempt from public records requests.

Timing of Notification

B23-215 currently requires that the D.C. Attorney General be notified prior to notifying an impacted resident of the breached information.[2] Several of our members are concerned that this requirement could unnecessarily delay an organization's response time. Data breach laws are most often designed to notify impacted customers of the breach so that they can take steps to protect themselves. The requirement to notify the AG first could delay the impacted customer notification, leaving them unable to take those protective measures. We believe that this is currently happening in both New Jersey and Maryland – the only two states we're aware of with a prior notification requirement. Should you choose not to expand the GLBA deemed-compliance provision to the AG notification, we urge you to consider simultaneous reporting.

On a separate but similar issue, there is no timing guidance included for entities that are required to provide consumer notices. We believe a general timing requirement would be helpful (e.g., "within a reasonable time after discovery and confirmation of a breach") but believe that any set timeframe of at least 45 days after discovery and confirmation of a breach would be beneficial.

De Minimis Requirement

Currently, this bill would require notification to the AG if certain information of any single D.C. resident was breached. This would be a fairly unique requirement that could lead to unnecessary reporting and additional burdens on both reporting entities and the District AG's Office. In other states that have a single resident requirement, the state agency notification is usually included in the deemed-compliance provision. Should you choose not to expand the GLBA deemed-compliance provision to the AG notification, we urge you to consider the addition of a de minimis requirement.[3]

Security Requirement

New Section 28-3852a would not require a greater level of security than what is already required by GLBA, but neither does it include identical requirements. Such regulatory inconsistency can take away from firm efforts to protect their customers. In fact, Firm cybersecurity staff are currently spending 40% of their time, on average, on regulatory compliance efforts, taking their time away from other cyber defense activities.[4] As such, we strongly suggest that the GLBA deemed-compliance provision be extended to include new Section 28-3852a's security requirements.

---

[2] Please note that clarification on the numbering of the sections may prove helpful; the proposed number (b-1) and (b-2) makes them appear to be part of the requirement to notify the owner or licensee of a breach, rather than the requirement to notify consumers.

[3] 500 or 1,000 residents are the two most common requirements.

[4] Financial Services Sector Coordinating Council, "Financial Services Sector Cybersecurity Recommendations," available at: fssc.org/files/galleries/FSSCC_Cybersecurity_Recommendations_for_Administration_and_Congress_2017.pdf.

- **The Definition of Personal Information Should Not Include "Attempt to Commit" Language**

  B23-215 currently includes any subset of information that would be sufficient for a person to "commit or attempt to commit identify theft […]" in subsection VII of the definition of "Personal Information." In this case, the "attempt to commit" language is both unnecessary and problematic. The entire subsection is already conditional (i.e., the definition includes information that "would be sufficient to commit […]") and would encompass the breach of any information which could cause harm to a consumer. On top of this, anyone could technically attempt to commit identity theft with any combination of information – regardless of whether such an attempt could ever be successful.

We appreciate your willingness to consider our suggestions. If there is any additional information we may be able to provide or any questions we can answer, please contact me at 212-313-1211 or kinnes@sifma.org with any questions.

Sincerely,

/s/
Kyle R. Innes
Assistant Vice President & Assistant General Counsel
SIFMA

CC: All Members, Committee of the Whole