SHENKER RUSSO & CLARK LLP

MEMORANDUM IN OPPOSITION

February 8, 2022

S.6701A – Thomas (ON CONSUMER PROTECTION COMMITTEE AGENDA, 2/8/22)
A.680B – Rosenthal, L. (In Consumer Affairs & Protection Committee)

AN ACT to amend the general business law, in relation to the management and oversight of personal data

This memorandum in ***opposition*** is written on behalf of our client, the New York Bankers Association (NYBA). NYBA is comprised of small, regional, and large banks across every region of New York State. Together NYBA members employ nearly 200,000 New Yorkers, safeguard $2 trillion in deposits, and annually extend nearly $70 billion in home and small business loans.

The New York Bankers Association opposes this legislation, the New York Privacy Act (NYPA) which, among other things, would require certain businesses to: collect opt-in consent before processing a consumer's personal data "for any purpose"; disclose and allow for an appeal when automated processes are used to make a decision related to financial services; conduct annual data protection assessments and purges of "unnecessary" data; and comply with a broad array of novel data-related rights given to consumers.

Unlike other industries, banks are already subject to a panoply of targeted, state and federal laws and comprehensive regulations that govern their handling of consumer data. Collectively these provisions impose on banks stringent data management, protection and privacy requirements which overlap with, and frequently encompass, the consumer protections advanced under NYPA. In particular, banks must already comply with the broad data privacy and disclosure requirements under the federal Gramm-Leach-Bliley Act of 1999 (GLBA),[1] which requires that financial institutions:

- secure consumer data through "administrative, technical, and physical safeguards;"
- annually notify consumers "clearly and conspicuously" of any data-sharing by the institution, and allow consumers to opt-out;
- limit the reuse and marketing of a consumer's information;
- refrain from fraudulently collecting or accessing consumer data; and
- implement a pro-active, as opposed to reactive, compliance regime.

[1] See, generally, 15 U.S.C. §§ 6801 – 6827.

These requirements are reinforced by fulsome enforcement provisions subjecting banks to potential penalties of up to $100,000 per violation, and individuals to potential penalties of up to $10,000 per violation. Individuals are also subject to criminal penalties, including up to 5 years in federal prison for an intentional violation, which may be increased to 10 years in aggravated cases.[2]

Given the strong, extensive and well-understood protections already applicable to banks under the GLBA, it is unsurprising that virtually all the legislative proposals currently under consideration by states regarding consumer data privacy either exempt financial institutions entirely (the "entity-based exemption"), or exempt certain categories of information commonly used by financial institutions (the "information-based exemption"). The "California Consumer Privacy Act" (CCPA) and the "Virginia Consumer Data Protection Act" (VCDPA) both include an exemption based on the application of the federal GLBA data protection provisions. Comparatively, California's privacy law provides the narrower information-level exemption, which has already shown itself as unclear regarding its scope.[3] Originally passed in 2018, CCPA is often utilized as a blueprint for other states in crafting consumer data privacy protections, however the original CCPA was amended and changed several times since then in efforts to address substantial confusion over its implementation. Financial institutions interpreting this exemption have had trouble puzzling out the final bill's intent and the distinctions created by its new formulation.[4] Given the many changes made to the California law over the years, it is notable that when Virginia legislators passed a pioneering privacy law in February of 2021, they expressly rejected an information-based exemption. Instead, the VCDPA incorporates an entity level exemption, which states that "[t]his chapter shall not apply to any . . . financial institutions or data subject to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.)."[5] This language is clear and financial institutions know exactly who and what is covered by the VCDPA.

Unfortunately, the NYPA's proposed exemption mirrors the California statute. It provides an information-based exemption for "personal data collected, processed, sold or disclosed pursuant to and in compliance with the federal Gramm- Leach-Bliley Act."[6] This

---

[2] 15 U.S.C. § 6823.

[3] See, *National Financial Institutions—Developing a Project Plan to Comply with the California Consumer Privacy Act*, Dorsey& Whitney LLP (June 28, 2019) ("Regrettably, considerable confusion exists within the financial industry about the scope of the CCPA and the obligations it imposes on financial institutions . . . On one hand, some industry stakeholders have argued that the GLBA Exemption excludes PI from virtually all requirements under the CCPA, while others have advocated that the exemption is very limited in scope, and specifically does not exclude financial institutions from obligations established by the CCPA that are not similar to those in the GLBA and the CFIPA.").

[4] See, Nicholas Farnsworth, Heather Egan Sussman, Emily Tabatabai and Shannon Yavorsky, *Wait…CCPA 2.0? What Is the California Privacy Rights Act of 2020 and Will It Become Law?*, JDSupra.com (May 20, 2020) ("[T]he CPRA may be seeking to narrow the interpretation of the financial information exception. Without further regulator guidance, it is difficult to predict the true impact this revision may have.") (https://www.jdsupra.com/legalnews/wait-ccpa-2-0-what-is-the-california-16687/)

[5] VCDPA § 59.1-572(B).

[6] 2022, NY Senate-Assembly Bill, S6701A, A680B (proposed GBS § 1101(2)(c)(1).

narrow exemption will create unnecessary ambiguity for consumers as well as significant increased implementation expenses for banks, without providing consumers with privacy standards that are materially more protective than those already required by GLBA. Given these issues, the New York Bankers Association respectfully requests an amendment that creates an entity-level exemption for financial institutions subject to GLBA.

In practice, determining whether an individual piece of information is protected under the CCPA or GLBA frequently depends on the reasons a financial institution is using it, making identical personal information exempt for some purposes but not for others.[7] Collection of a datum may be covered under one statute, but its disclosure or processing governed by another. Events of the same type may even be controlled by different statutes; for example, one processing event may be subject to the GLBA while a subsequent one is governed by the CCPA. Adopting California's GLBA exemption will subject New York businesses to the same conundrum and require them to engage in the same fraught line-drawing exercises.[8] Understandably, there will be marginal cases where reasonable people will disagree, but NYPA would set high stakes on nuanced interpretation, because any error—even a reasonable one—might encourage frivolous class action suits. Privacy laws that penalize so erratically make the state an even more unwelcoming environment in which to do business. Simply by patterning its GLBA exemption after the Virginia statute, the NYPA could eliminate these consequences.

An entity-level exemption would also give bank consumers what they really deserve: a uniform, comprehensive and consistent right to privacy over their financial information that will not vary from state to state. This is particularly relevant in an evolving commercial landscape where consumers are more mobile than ever, financial and account transactions can touch multiple jurisdictions. Under these circumstances, the inevitable confusion over which jurisdiction's data protection laws apply can be avoided with a stable and dependable standard. One virtue of Title V of GLBA is that it is a federal law and applies uniformly in the U.S. no matter where a consumer or their data travels.

Lastly, if NYPA does not provide an entity-level exemption for financial institutions, its ambiguous GLBA information-based exemption will distract New York regulators from the real abuses NYPA seeks to address, per the sponsor's memo. It is clear

[7] *Exempt or Not Exempt? California Consumer Privacy Act and the Gramm-Leach-Bliley Act*, Davis Wright Tremaine LLP (April, 15, 2019) ("Financial services businesses should review their data inventories carefully and make determinations as to what information is subject to CCPA at the data flow and data element level. . . . [T]he same data elements—such as name, email address, and IP address—may be exempt in one situation and not in another.") (https://www.dwt.com/blogs/privacy--security-law-blog/2019/04/exempt-or-not-exempt).

[8] See, *State Privacy Laws Must Include an Entity Level Exception for Financial Institutions Subject to GLBA*, AMERICAN BANKERS ASSOCIATION (January 27, 2020) (discussing imprecision of the similarly worded GLBA exemption in the CCPA: "Industry is currently undertaking substantial efforts to comply with CCPA. However, every review reveals additional unintended challenges and raises a number of questions. Due to this confusion, it may take years before both industry and regulators have a firm grasp on the full impact of CCPA.").

SHENKER RUSSO & CLARK LLP

that NYPA's primary objective is to reign in other actors that are virtually unregulated. An entity-level exemption is a sensible approach as financial institutions' data practices are already governed by GLBA and other federal statutes.

For these reasons, the New York Bankers Association **opposes** this legislation and urges that it be **held**.

Respectfully Submitted,

SHENKER RUSSO & CLARK LLP