Summary of Rep. McHenry Draft Privacy Proposal

In 1999, Congress passed and President Clinton signed the Gramm-Leach-Bliley Act (GLBA), a comprehensive and sweeping financial services reform law. Title V set forth a series of privacy and data security requirements for financial institutions (including insurers and insurance producers) that remain in place today. GLBA adopted a framework in which the various functional financial services regulators adopt and enforce privacy requirements as outlined in the law.

Title V has only been revised in modest ways over the years, and many policymakers in Congress and at the state level believe privacy requirements have not kept up with the marketplace changes and technology revolution of the last two decades. Many have called for the adoption of more robust privacy protections in the financial services world and beyond. Several federal privacy proposals have been introduced in recent years, and California and four other jurisdictions have enacted comprehensive privacy legislation at the state level since 2018 (with more such statutes expected). In addition, the NAIC intends to produce a potentially troubling insurance industry-specific privacy model in 2023, and an initial discussion draft of that proposal is expected to be released by the end of January.

Representative Patrick McHenry (R-NC), the new chairman of the House Financial Services Committee, unveiled draft legislation that would revise GLBA Title V and address privacy in the financial services world in mid-2022. His prominent position in the new Congress and the increased focus on privacy issues in general means that discussion and consideration of the McHenry proposal is expected to now gather steam. Although this proposal is likely to evolve and be revised, below are some of the most notable elements contained in the discussion draft previously released:

- **Continued Application of the GLBA Privacy Framework to the Insurance Industry** – The draft relies on the existing GLBA structure, which means any insurance industry rules and standards adopted pursuant to revisions made to the law would be enforced by state insurance regulators. Although the discussion draft would apply to insurers and insurance producers, the extent to which any new privacy-related legislation should extend to the insurance industry is a subject that will be discussed in more detail in the weeks to come.

- **Privacy Policy Disclosure** – The draft would revise existing privacy policy disclosure obligations, which currently require institutions to disclose a description of the categories of nonpublic personal information that are collected and the manner in which such information is shared with affiliates and other entities. The proposal would require financial institutions to also disclose the purpose for collecting the information, how the information will be used, their data retention policies, and the existence of the new consumer rights that are outlined in greater detail below.

- **Consumer Ability to Opt Out** – The proposal would prohibit a financial institution from collecting or sharing nonpublic personal information with nonaffiliated third parties unless the consumer is given the opportunity to stop collection or further disclosure.[1] If a consumer

[1] The notice and opt out provisions of the bill would not prevent financial institutional institutions from collecting nonpublic personal information or disclosing it to nonaffiliated third parties in certain instances, including when the collection or disclosure is necessary to provide a product or service requested or authorized by the consumer. The bill would similarly allow the sharing of nonpublic personal information

directed a financial institution not to share nonpublic personal information with a nonaffiliated third party, then the financial institution would be required to notify the third party that the sharing has been terminated and the third party may no longer share any information about the consumer.

- **New Consumer Rights** – The draft would enable consumers to get access to their nonpublic personal information and to demand its deletion. It would require a financial institution, upon request, to disclose the nonpublic personal information about a person that it holds, a list of nonaffiliated third parties it has shared the information with, and a list of the nonaffiliated third parties from whom it has received any nonpublic personal information about the person. Consumers would also be able to request the deletion of their data, and a financial institution would be required to do so unless retention of the information by the institution is required by other law.

- **Impact on Small Businesses** – The draft would direct financial services regulators to take into account the compliance costs any proposed new rules issued pursuant to GLBA would impose on small institutions.

- **Preemption of State Law** – The draft would preempt certain categories of state laws in an effort to achieve national uniformity in this area for financial institutions. The types of state laws that would be preempted include those that address the collection of nonpublic personal information, the disclosure of privacy policies, and consumer access to and deletion of nonpublic personal information.

- **Liability** – The draft would make a financial institution liable to consumers for "the full amount of any damages" that arise if nonpublic personal information is obtained from the institution as a result of a breach or in any other manner and is used to gain unauthorized access to the consumer's account.

- **"Nonpublic Personal Information" Definition** – Protection of "nonpublic personal information" would remain the focus of the GLBA framework. The proposal would revise the existing definition to mean "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer" that is (1) provided by a consumer to a financial institution, (2) a result of a transaction with or service provided to a consumer, or (3) otherwise obtained by the institution. The term would continue to exclude "publicly available information."

- **Data Aggregators** – The draft bill's requirements would apply to data aggregators in the same manner as financial institutions. The term "data aggregator" would be defined to include most entities that are in the business of "accessing, aggregating, collecting, selling, or sharing nonpublic personal information about consumer financial accounts or transactions at the direction of a consumer."

---

with nonaffiliated third parties who perform services for or on behalf of financial institutions if those third parties enter into a contract that requires them to maintain the confidentiality of the information.