VERMONT

DEPARTMENT OF FINANCIAL REGULATION

H.121: ENHANCING CONSUMER PRIVACY

February 6, 2024

OVERVIEW OF KEY POINTS

- DFR has a shared goal of protecting consumer data
- DFR's regulated entities are already subject to a number of laws and rules related to data privacy and protection of consumer information. DFR, independently and through its membership in national associations, has worked on consumer privacy issues for years and this is a regulated area.
- Our goal in assessing this bill is to avoid confusion and to ensure that entities/areas that are already regulated are not subject to conflicting requirements.
- We appreciate the recognition of existing frameworks in the exemptions section of the bill, which includes exemptions relating to data covered by HIPAA, Gramm Leach Bliley, DFR's Privacy of Consumer Financial and Health Information Regulations, financial institutions, and insurers and producers.
  - We are still assessing the language of these exemptions and how they match up to our existing laws. We anticipate having some suggested language to clarify exemptions and would like to follow up with legislative counsel or written testimony.
  - One clarification we hope to make clear is that captive insurance is included with the entity-level exemption for insurers by adding reference to 8 VSA 6001(5) in 2417(a)(13) on page 16.

DFR RULES FOR DATA PRIVACY

- DFR Privacy of Consumer Financial and Health Information
- Reg IH-2001-0 and Reg B-2018-01
- Link: https://dfr.vermont.gov/sites/finreg/files/regbul/dfr-regulation-insurance-IH-2001-01.pdf and https://dfr.vermont.gov/sites/finreg/files/regbul/dfr-regulation-b-2018-01.pdf
- These regulations govern the treatment of nonpublic personal financial information and nonpublic personal health information about individuals by insurance and banking licensees. The regulations: (1) Require a licensee to provide notice to individuals about its privacy policies and practices; (2) Describe the conditions under which a licensee may disclose nonpublic personal financial information and nonpublic personal health information about individuals to nonaffiliated third parties; and (3) Require licensees to obtain consumer consent prior to disclosing that information, subject to the exceptions in sections 14, 15, 16, and 17 of this regulation and subject to the federal Fair Credit Reporting Act and Vermont Fair Credit Reporting Act.

DFR RULES FOR DATA PRIVACY

- Regulation I-2002-03: Standards for Safeguarding Consumer Information
- In place since 2003
- Link: https://dfr.vermont.gov/reg-bul-ord/standards-safeguarding-customer-information
- The regulation establishes standards for developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information, consistent with GLB. It includes, among other topics, standards relating to information security programs, risk assessments, and oversight of third parties.

8 VSA 4728: VERMONT INSURANCE DATA SECURITY LAW

- Link: https://legislature.vermont.gov/statutes/section/08/129/04728
- This section establishes the exclusive State standards applicable to licensees for data security and for the investigation of a cybersecurity event.
- Adopted in 2021 and amended in 2023

ONGOING NAIC WORK

- The Privacy Protections (H) Working Group is charged with drafting a new model law to replace the existing models. The group is currently engaged in the drafting process for the new Privacy Protections Model Act (#674). The model covers several topics including consumer rights, consent, and notification as well as third-party service agreements, data retention and deletion policies, and data sharing agreements. The working group is taking a collaborative approach to the drafting process and collecting feedback from various stakeholders, including consumer and industry representatives. The current draft of the model can be found on the exposure drafts tab of the working group's webpage. The working group is re-evaluating the timeline for this project to carefully consider feedback from all interested parties.

GRAMM LEACH BLILEY

- Applies to banks, trust companies, credit unions, various financial entities, brokers, dealers, and people providing insurance services, including investment companies and investment advisors.
- GLBA is a privacy framework for financial institutions. GLBA's mandate includes two major protections: a) comprehensive information security requirements; and b) privacy notice obligations and information sharing restrictions.
- GLBA requires financial institutions to establish an information security program that protects customer information through safeguards that are appropriate to the size and complexity of the financial institution and the nature and scope of its activities.
- Requires financial institutions to provide consumers with a privacy notice that clearly and conspicuously describes the financial institution's privacy policy and practices, including the circumstances under which it shares personal information about consumers and how it protects personal information. GLBA generally prohibits financial institutions from disclosing financial and other consumer information to nonaffiliated third parties without first providing consumers with notice and a reasonable opportunity to opt-out of such sharing. GLBA also includes carefully crafted exceptions to its restrictions on sharing information with nonaffiliated third parties to ensure financial institutions can run their businesses effectively and safely protect consumers.