VERMONT
DEPARTMENT OF FINANCIAL REGULATION
89 Main Street, Montpelier, VT 05620 - 3101
(p) 802-828-3301 | http://www.dfr.vermont.gov/

MEMORANDUM

TO: House Committee on Commerce and Economic Development
FROM: Department of Financial Regulation
SUBJECT: H.B. 121 Version 7.1 – Exemptions related to DFR Regulated Entities
DATE: February 29, 2024

The Department of Financial Regulation (the "DFR") has reviewed changes to the exemptions included in H.B. 121, Version 7.1. Through this review, the DFR has identified several areas where small changes could support the data-level exemptions sought by the Committee while avoiding duplicative regulation of entities regulated by the DFR.

I. General Observations

With the focus on data-level exemptions, some of the personal data collected by DFR licensees, and their use of such data, would be subject to the provisions of the proposed law. To the extent the Committee maintains focus on data-level exemptions, the DFR requests that it be given jurisdiction over implementation and enforcement of the law for DFR licensees. As DFR has broad examination and enforcement authority it will be in the best position to learn of noncompliance with H.B. 121. Additionally, violations of the proposed law may be accompanied with violations of DFR statues and rules. At a minimum, DFR should be involved in the investigation and enforcement of H.B. 121 by the AGO against DFR licensees.

For improved consistency, the DFR suggests that the exemption section utilize the defined terms included in Section 2415. By way of example, the term "individual" could be changed to the defined term "consumer." The term "information" could be changed to the defined term "personal data" and, at times, the term "business entity" could be changed to "controller" and "processor."

A final general observation is that some of the individual rights provided in H.B. 121 appear to conflict with the nature of financial entities, including the business of insurance. The right to delete records is a good example of this concern. A wide range of state and federal financial laws require retention of accurate records to prevent misconduct and fraud by and against financial entities, and allow for investigation and examination of such entities and their employees, customers, etc. These include a variety of state and federal securities laws, banking laws, anti-money laundering, anti-terrorism, and "know-your-client" rules. The ability to alter or delete information held by financial entities would both interfere with the ordinary course of

business and could interfere with regulatory oversight and criminal investigations. Regulation of financial entities is unlikely to be the only arena in which laws exist which prevent regulated entities from deleting records. The committee could consider adding an express step to the denial process in 9 V.S.A. § 2418(c)(2) that requires a controller, when denying a request to delete data because a law prohibits it from doing so, to cite to the specific law and clarify that the law prevents deletion, so that requestors are made aware of the reason for a denial.

II. Exemptions

After reviewing the proposed data-level exemptions, the DFR proposes the following changes.

1. **2417(a)(2)**:

The following are proposed changes to the existing language in Section 2417(a)(2). It is unclear why only IH-2001-01 is listed in this section and not similar regulations impacting the Banking and Securities Divisions that also pertain to nonpublic personal health information. *See* B-2018-01 (Banking Division: Privacy of Consumer Financial and Health Information); Docket No. 16-01-S (Securities Division: Privacy of Consumer Financial and Health Information).

a. Edit citation to read IH-2001-01. Currently the citation includes a typo; it uses 1 in place of I -- "1H-2001-01." This same typo is found in Section 2417(a)(11)(G).
b. This exemption currently states that "protected health information that a covered entity or business associate" processes in accordance with IH-2001-1 is exempt. IH-2001-01, and the substantially similar regulations by the Banking and Securities Division, do not use these terms. As a result, the exemption as drafted could create confusion as to what information is exempt.
c. Proposed edits for Section 2417(a)(2): "protected health information or consumer health data that a ~~covered entity or business associate~~ collector or processor collects or processes in accordance with, or documents that a ~~covered entity or business associate~~ collector or processor creates for the purpose of complying with:

. . .

(B) Vermont Regulation ~~1~~IH-2001-01 (Privacy of Consumer Financial and Health Information ~~Regulation~~);

(C) Vermont Regulation B-2018-01 (Privacy of Consumer Financial and Health Information Regulation);

(D) Department of Financial Regulation, Securities Division, Docket No. 16-01-S, *In the matter of: Repealing in part and retaining in part Order 06-23-S Applying Provisions of Certain Regulations, Bulletins, Policy Statement and order in effect Prior to July 1, 2006 to the Vermont Uniform Securities Act*, as may be amended or adopted through rulemaking;

2. **2417(a)(8)**

Subsection 2417(a)(8) describes the entities that could hold the relevant data as "covered entity, business associate, or a qualified service organization program." As noted in the previous section, this reference leaves out the wider entities regulated by IH-2001-01, and the substantially similar regulations by the Banking and Securities Division. It also may leave out other entities regulated by the federal provisions listed in (a)(2)-(7).

a. This provision could read: "information that originates from, or that is intermingled so as to be indistinguishable from, information described in subdivisions (2) through (7) of this subsection (a) that a ~~covered entity, business associate, or a qualified service organization program~~ controller or processor creates, collects, processes, uses, or maintains in the same manner as is required under the laws, regulations, and guidelines described in subdivisions (2) through (7) of this subsection;"

3. **2417(a)(11)**:

Subsection (a)(11) states that "information collected, processed, sold, or disclosed under and in accordance with the following laws and regulations" are exempt.[1] While the intent of (11) appears to be to exempt information regulated pursuant the listed laws and regulations, the introductory phrase has ambiguity that will be problematic to both regulators and regulated entities unless the language is modified or rulemaking accompanies the legislation.

The ambiguity resides principally with the use of information "collected, processed, sold or disclosed under and in accordance with" in the introductory phrase. This language implies that a level of analysis may be necessary that delves beyond what information is governed by a particular law or regulation in order to determine how the exemption applies. If this language was replaced with information "subject to" it is far clearer what the intent is – that so long as the information is being regulated under the listed laws and regulations, it is exempt. Without clarification the potential for an array of divergent interpretations exists.

a. Proposed edits for Section 2417(a)(11):To add the most clarity, the introductory phrase to subsection (a)(11) could read "~~information collected, processed, sold or disclosed under and in accordance to~~ personal data subject to the following laws and regulations:"

In addition to the comments above, the DFR recommends adding a reference to the Securities Division's equivalent of IH-2001-01 and B-2018-01. For Securities this is DFR Order Docket No. 16-01-S. This Order clarifies that Exhibit 5.11 the Privacy of Consumer Financial and Health Information provisions remain in effect as to securities.

b. Proposed addition (which may be altered if any changes are made based on the preceding paragraph): Department of Financial Regulation, Securities Division,

[1] Note also that "process" is defined to mean "means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data." This means that the list provided in this section is both redundant and under inclusive of the full definition of "process."

Docket No. 16-01-S, *In the matter of: Repealing in part and retaining in part Order 06-23-S Applying Provisions of Certain Regulations, Bulletins, Policy Statement and order in effect Prior to July 1, 2006 to the Vermont Uniform Securities Act*, as may be amended or adopted through rulemaking.

4. **2417(a)(12)**

This subsection states that "information that originates from, or is intermingled so as to be indistinguishable from, information described in subdivision *(11)(A)* of this subsection and that *a licensee for consumer finance loans* collects, processes, uses, or maintains in the same manner as is required under the laws and regulations specified in subdivision *(11)(A)* of this subsection." (emphasis added). It is not clear to the DFR why this exemption would only be limited to licensees who provide consumer loans – one specific DFR-regulated entity – because GLBA applies to far more entities.

It appears that this exemption is a mirror of 2417(a)(8) and could be intended to create an exemption for information that is intermingled with the heavily regulated information already exempted pursuant to 2417(a)(11)(A)-(H). This would be a logical exemption as any information intermingled with information in (a)(11)(A)-(H) is protected by the same laws and regulations that warranted exemptions of the regulated data. To accomplish this objective for 2417(a)(12), the exemption should cite the full range of laws and regulations under 2417(a)(11) as well as the entities that may be impacted by those laws or regulations.

a. Proposed revision: "information that originates from, or is intermingled so as to be indistinguishable from, information described in subdivisions (11)(A)-(H) of this subsection and that a ~~licensee for consumer finance loans~~ controller or processor collects, processes, uses, or maintains in the same manner as is required under the laws and regulations specified in subdivisions (11)(A)-(H) of this subsection;"
b. Alternatively, if the exemption is intended to only pertain to licensees who provide consumer loans, the term "licensee for consumer finance loans" should be replaced with the term "lender licensed pursuant to Title 8, Chapter 73" and the subdivisions of exemption 11 expanded to include (11)(A) and (H).

5. **9 V.S.A. § 2417(a)(14)**

This exemption is ambiguous as currently written because it uses the term "financial institution," a term used to mean entirely different things in different contexts, and is language borrowed from Oregon which uses the term differently than the DFR. To maintain its intended scope – chartered banks and credit unions and similar chartered institutions – it should be modified in the following way.

a. Proposed revision: "a financial institution as defined in in subdivision 11101(32) of title 8, a credit union as defined in subdivision 30101(5) of title 8, an independent trust company as defined in subdivision 2401(3) of title 8, or an ~~financial institution's~~ affiliate or subsidiary thereof that is only and directly engaged in financial activities, as described in 12 U.S.C. § 1843(k);"