9 V.S.A. chapter 62 – Protection of Personal Information	H.515 – Commerce Draft 1.2 – Sec. 20
§ 2430 - Definitions	§ 4728(c) – Definitions
(10)(A) "Personally identifiable information" means a consumer's first name or first initial and last name in combination with one or more of the following digital data elements, when the data elements are not encrypted, redacted, or protected by another method that renders them unreadable or unusable by unauthorized persons: (i) a Social Security number; (ii) a driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction; (iii) a financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords; (iv) a password, personal identification number, or other access code for a financial account; (v) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data; (vi) genetic information; and (vii)(I) health records or records of a wellness program or similar program of health promotion or disease prevention; (II) a health care professional's medical diagnosis or treatment of the consumer; or (III) a health insurance policy number.	(9) "Nonpublic information" means information that is not publicly available information and is: (A) business-related information of a licensee, the tampering with which, or unauthorized disclosure, access, or use of which would cause a material adverse impact to the business, operations, or security of the licensee; (B) information concerning a consumer that, because of name, number, personal mark, or other identifier, can be used to identify such consumer, in combination with any one or more of the following data elements: (i) Social Security number; (ii) driver's license number or nondriver identification card number; (iii) individual taxpayer identification number; (iv) passport number; (v) military identification card number; (vi) financial account number or credit or debit card number; (vii) security code, access code, or password that would permit access to a consumer's financial account; or (viii) biometric record; (C) information or data, except age or gender, in any form or medium created by or derived from a health care provider or a consumer, that relates to: (i) the past, present, or future physical, mental, or behavioral health or condition of any consumer or a member of the consumer's family; (ii) the provision of health care to any consumer; or (iii) payment for the provision of health care to any consumer.

(B) "Personally identifiable information" does not mean publicly available information that is lawfully made available to the general public from federal, State, or local government records.	(10)(A) "Publicly available information" means information that a licensee has a reasonable basis to believe is lawfully made available to the general public from federal, state, or local government records, widely distributed media, or disclosures to the general public that are required to be made by federal, state, or local law. (B) As used in this subdivision, a licensee has a "reasonable basis to believe" that information is lawfully made available to the general public if the licensee has taken steps to determine: (i) that the information is of the type that is available to the general public; and (ii) whether a consumer can direct that the information not be made available to the general public and, if so, that the consumer has not done so.
§ 2430 - Definitions (13)(A) "Security breach" means unauthorized acquisition of electronic data, or a reasonable belief of an unauthorized acquisition of electronic data, that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information or login credentials maintained by a data collector. (B) "Security breach" does not include good faith but unauthorized acquisition of personally identifiable information or login credentials by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personally identifiable information or login credentials are not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure. (C) In determining whether personally identifiable information or login credentials have been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data collector may consider the following factors, among others: (i) indications that the information is in the physical possession and control of a person without valid	§ 4728(c) – Definitions (3) "Cybersecurity event" means an event resulting in unauthorized access to or disruption or misuse of an information system or nonpublic information stored on such information system. The term "cybersecurity event" does not include: (A) the unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization; or (B) an event with regard to which the licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

authorization, such as a lost or stolen computer or other device containing information; (ii) indications that the information has been downloaded or copied; (iii) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or (iv) that the information has been made public.	