

State of Vermont
Department of Financial Regulation
Banking Division

REGULATION B-2018-01
PRIVACY OF CONSUMER FINANCIAL AND
HEALTH INFORMATION REGULATION

(This Regulation replaces Regulation B-2015-02)

Table of Contents

ARTICLE I. GENERAL PROVISIONS

- Section 1. Authority
- Section 2. Purpose; Scope; Application; Compliance Rule; Exception for Information about Business Customers
- Section 3. Rule of Construction
- Section 4. Definitions

ARTICLE II. PRIVACY AND OPT IN NOTICES FOR NONPUBLIC PERSONAL
INFORMATION

- Section 5. Initial Privacy Notice to Consumers Required
- Section 6. Annual Privacy Notice to Customers Required
- Section 7. Information to be Included in Privacy Notices
- Section 8. Form of Opt In Notice to Consumers and Opt In Methods
- Section 9. Revised Privacy Notices
- Section 10. Delivery

ARTICLE III. LIMITS ON DISCLOSURES OF FINANCIAL INFORMATION

- Section 11. Limitation on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties
- Section 12. Limits on Redisclosure and Reuse of Nonpublic Personal Financial Information
- Section 13. Limits on Sharing Account Number Information for Marketing Purposes

ARTICLE IV. EXCEPTIONS TO LIMITS ON DISCLOSURES OF INFORMATION

- Section 14. Exception for Disclosure of Nonpublic Personal Information for Service Providers and Joint Marketing
- Section 15. Exceptions to Notice and Opt In Requirements for Disclosure of Nonpublic Personal Financial Information for Processing and Servicing Transactions
- Section 16. Other Exceptions to Notice and Opt In Requirements for Disclosure of Nonpublic Personal Financial Information

ARTICLE V. RULES FOR HEALTH INFORMATION

- Section 17. When Authorization Required for Disclosure of Nonpublic Personal Health Information
- Section 18. Authorizations
- Section 19. Authorization Request Delivery
- Section 20. Relationship to Federal Rules
- Section 21. Relationship to State Laws

ARTICLE VI. ADDITIONAL PROVISIONS

- Section 22. Protection and Application of Fair Credit Reporting Acts
- Section 23. Nondiscrimination
- Section 24. Violations
- Section 25. Severability
- Section 26. Effective Date

Appendix A –Sample Clauses

ARTICLE I. GENERAL PROVISIONS

Section 1. Authority

This regulation is promulgated pursuant to the authority granted by 8 V.S.A. §§ 10, 15, 2214, 2766, 2914, 10201 *et seq.*, and 30203.

Section 2. Purpose; Scope; Application; Compliance rules; Exception for Information about business customers

A. Purpose. This regulation governs the treatment of nonpublic personal information about consumers by the financial institutions listed in subsection C of this section. This regulation:

- (1) Requires a financial institution to provide notice to individuals about its privacy policies and practices;
- (2) Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties;
- (3) Requires financial institutions to obtain consumer consent prior to disclosing that information, subject to the exceptions in Sections 14, 15, 16 and 17 of this regulation and 8 V.S.A. § 10204 and subject to the federal Fair Credit Reporting Act and Vermont Fair Credit Reporting Act; and,
- (4) Provides an exemption from the provisions of 8 V.S.A. §§ 10201 *et seq.* for information about business customers.

B. Scope. This regulation applies to: (1) nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes from the institutions listed below; and (2) all nonpublic personal health information. This regulation does not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural purposes, other than for the purpose of establishing an exemption from the provisions of 8 V.S.A. §§ 10201 *et seq.* for information of business customers.

C. Application. This regulation applies to the following:

- (1) financial institutions within the meaning of 8 V.S.A. § 10202 (5);
- (2) any person required to be licensed or registered with the commissioner under Part 2 of title 8 V.S.A.;
- (3) lenders, mortgage brokers, sales finance companies, and mortgage loan originators subject to chapter 73 of title 8 V.S.A.;
- (4) independent trust companies subject to chapter 77 of title 8 V.S.A.;

- (5) money services providers under chapter 79 of title 8 V.S.A.;
- (6) debt adjusters under chapter 83 of title 8 V.S.A.;
- (7) loan servicers under chapter 85 of title 8 V.S.A.;
- (8) branches and agencies of foreign banks; and,
- (9) any subsidiaries of such entities; provided, however, that this regulation does not apply to any subsidiary that is subject to a privacy law or rule implementing Title 15 U.S.C. § 6801 et seq. and is not a financial institution within the meaning of 8 V.S.A. § 10202 (5).

D. *Compliance rule.* A person subject to this regulation, regardless of its jurisdiction of domicile, shall comply with the provisions of this regulation for transactions with Vermont consumers.

E. *Exception for information about business customers.* The disclosure of financial information by a financial institution about any business customer is exempt from the prohibition in the Vermont Financial Privacy Act, 8 V.S.A. § 10203, on the disclosure of financial information relating to a customer. This exception is not intended to limit or supersede the applicability of any other state or federal law or rule that might otherwise apply to the disclosure of information relating to a business customer. For purposes of this regulation, “business customer” means any person, whether an individual or entity, that obtains a financial product or service that is not primarily for personal, family, or household purposes, including a surety or guarantor of a loan that is not made primarily for personal, family, or household purposes.

Section 3. Rule of Construction for Examples and Appendix A

The examples in this regulation and the sample clauses in Appendix A of this regulation are not exclusive. The examples in this regulation and the sample clauses in the Appendix of this regulation provide guidance concerning the regulation’s application in ordinary circumstances. The facts and circumstances of each individual situation, however, will determine whether compliance with an example or use of a sample clause, to the extent applicable, constitutes compliance with this regulation.

Section 4. Definitions

As used in this regulation, unless the context requires otherwise:

A. “*Affiliate*” shall have the same meaning as in 8 V.S.A. § 11101 (1). The term affiliate shall also include a credit union service organization as defined in 12 U.S.C. Section 712 which is controlled by, or of which 67 % or more is owned by, a credit union or credit unions.

B. (1) “*Clear and conspicuous*” means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) *Examples.*

(a) *Reasonably understandable.* A financial institution makes its notice reasonably understandable if it:

- (i) Presents the information in the notice in clear, concise sentences, paragraphs, and sections;
- (ii) Uses short explanatory sentences or bullet lists whenever possible;
- (iii) Uses definite, concrete, everyday words and active voice whenever possible;
- (iv) Avoids multiple negatives;
- (v) Avoids legal and highly technical business terminology whenever possible;
- (vi) Avoids explanations that are imprecise and readily subject to different interpretations; and
- (vii) Avoids contradictory, confusing or misleading language.

(b) *Designed to call attention.* A financial institution designs its notice to call attention to the nature and significance of the information in it if the financial institution:

- (i) Uses a plain-language heading to call attention to the notice;
- (ii) Uses a typeface and type size that are easy to read;
- (iii) Provides wide margins and ample line spacing;
- (iv) Uses boldface or italics for key words; and
- (v) In a form that combines the financial institution's notice with other information, uses distinctive type size, style, and graphic devices, such as shading or sidebars.

(3) *Notices on web sites.* If a financial institution provides a notice on a web page, the financial institution designs its notice to call attention to the nature and significance of the information in it if the financial institution uses text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice, and the financial institution either:

- (a) Places the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or
- (b) Places a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature, and relevance of the notice.

C. “*Collect*” means to obtain information that the financial institution organizes or can retrieve by the name of an individual or by identifying number, symbol, or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

D. “*Commissioner*” means the commissioner of the Department of Financial Regulation.

E. “*Company*” means any corporation, limited liability company, business trust, general or limited partnership, association, sole proprietorship or similar organization.

F. (1) “*Consumer*” means an individual who seeks to obtain, obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.

(2) *Examples.*

(a) An individual who applies to a financial institution for credit for personal, family, or household purposes is a consumer of a financial service, regardless of whether the credit is extended.

(b) An individual who provides nonpublic personal information to a financial institution in order to obtain a determination about whether he or she may qualify for a loan to be used primarily for personal, family, or household purposes is a consumer of a financial service, regardless of whether the loan is extended.

(c) An individual who provides nonpublic personal information to a financial institution in connection with obtaining or seeking to obtain financial, investment, or economic advisory services is a consumer regardless of whether the financial institution establishes a continuing advisory relationship.

(d) If a financial institution holds ownership or servicing rights to an individual's loan that is used primarily for personal, family, or household purposes, the individual is the financial institution's consumer, even if the financial institution holds those rights in conjunction with one or more other institutions. (The individual is also a consumer with respect to the other financial institutions involved.) An individual who has a loan in which a financial institution has ownership or servicing rights is the financial institution's consumer, even if the financial institution, or another institution with those rights, hires an agent to collect on the loan.

(e) An individual who is a consumer of another financial institution is not a financial institution's consumer solely because the financial institution acts as agent for, or provides processing or other services to, that financial institution.

(f) An individual is not a financial institution's consumer solely because he or she has designated the financial institution as trustee for a trust.

(g) An individual is not a financial institution's consumer solely because he or she is a beneficiary of a trust for which the financial institution is a trustee.

(h) An individual is not a financial institution's consumer solely because he or she is a participant or a beneficiary of an employee benefit plan that the financial institution sponsors or for which the financial institution acts as a trustee or fiduciary.

G. “*Consumer reporting agency*” has the same meaning as in Section 603(f) of the Fair Credit Reporting Act (15 U.S.C. § 1681a(f)) and shall include any “credit reporting agency” within the meaning of 9 V.S.A. § 2480a (3).

H. “*Control*” has the same meaning as in 8 V.S.A. § 11101 (17).

I. “*Customer*” means a consumer who has a customer relationship with a financial institution.

J. (1) “*Customer relationship*” means a continuing relationship between a consumer and a financial institution under which the financial institution provides one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.

(2) *Examples.*

(a) *Continuing relationship.* A consumer has a continuing relationship with a financial institution if the consumer:

(i) Has a deposit or investment account with the financial institution;

(ii) Obtains a loan from the financial institution;

(iii) Has a loan for which the financial institution owns the servicing rights;

(iv) Purchases an insurance product from the financial institution;

(v) Holds an investment product through the financial institution, such as when the financial institution acts as a custodian for securities or for assets in an Individual Retirement Arrangement;

(vi) Enters into an agreement or understanding with the financial institution whereby the financial institution undertakes to arrange or broker a home mortgage loan for the consumer;

(vii) Enters into a lease of personal property with the financial institution; or

(viii) Obtains financial, investment, or economic advisory services from the financial institution for a fee.

(b) *No continuing relationship.* A consumer does not, however, have a continuing relationship with a financial institution if:

- (i) The consumer obtains a financial product or service only in isolated transactions, such as using the financial institution's ATM to withdraw cash from an account at another financial institution or purchasing a cashier's check or money order;
- (ii) The financial institution sells the consumer's loan and does not retain the rights to service that loan; or
- (iii) The financial institution sells the consumer airline tickets, travel insurance, or traveler's checks in isolated transactions.

K. (1) “*Financial institution*” means any entity the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. § 1843(k)), including:

- (a) a financial institution within the meaning of 8 V.S.A. § 10202 (5);
- (b) any person required to be licensed or registered with the commissioner under Part 2 of title 8, V.S.A., and the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. § 1843(k));
- (c) lenders, mortgage brokers, sales finance companies, and mortgage loan originators subject to chapter 73 of title 8 V.S.A.;
- (d) independent trust companies under chapter 77 of title 8 V.S.A.;
- (e) money services providers under chapter 79 of title 8 V.S.A.;
- (f) debt adjusters under chapter 83 of title 8 V.S.A.;
- (g) loan servicers under chapter 85 of title 8 V.S.A.;
- (h) branches and agencies of foreign banks; and,
- (i) any subsidiaries of such entities.

(2) *Financial institution does not include:*

- (a) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. § 1 et seq.);
- (b) The Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971 (12 U.S.C. § 2001 et seq.); or

(c) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights), or similar transactions related to a transaction of a consumer, as long as such institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.

L. (1) “*Financial product or service*” means any product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. § 1843(k)).

(2) Financial service includes a financial institution's evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.

M. “*Health care*” means:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, services, procedures, tests or counseling that:

(a) Relates to the physical, mental or behavioral condition of an individual; or

(b) Affects the structure or function of the human body or any part of the human body, including the banking of blood, sperm, organs or any other tissue; or

(2) Prescribing, dispensing or furnishing to an individual drugs or biologicals, or medical devices or health care equipment and supplies.

N. “*Health care provider*” means a physician or other health care practitioner licensed, accredited or certified to perform specified health services consistent with state law, or a health care facility.

O. “*Health information*” means any information or data except age or gender, whether oral or recorded in any form or medium, created by or derived from a health care provider or the consumer that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of an individual;

(2) The provision of health care to an individual; or

(3) Payment for the provision of health care to an individual.

Nothing in this definition shall preclude the disclosure of health information by a financial institution as necessary to process payments for the provision of health care to an individual. This definition does not require the segregation, nor does it prohibit the aggregation, of

information relating to the processing of payments for the provision of health care to an individual and information concerning payments processed for any other reason.

P. (1) “*Nonaffiliated third party*” means any person except:

(a) A financial institution's affiliate; or

(b) A person employed jointly by a financial institution and any company that is not the financial institution's affiliate (but nonaffiliated third party includes the other company that jointly employs the person).

(2) Nonaffiliated third party includes any company that is an affiliate solely by virtue of a financial institution's (or its affiliate's) direct or indirect ownership or control of the company in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) of the Bank Holding Company Act of 1956 and 8 V.S.A. § 12603 or insurance company investment activities of the type described in Section 4(k)(4)(I) of the Bank Holding Company Act of 1956 (12 U.S.C. § 1843(k)(4)(H) and (I)).

Q. “*Nonpublic personal information*” means nonpublic personal financial information and nonpublic personal health information.

R. (1) “*Nonpublic personal financial information*” means:

(a) Personally identifiable financial information; and

(b) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

(2) *Nonpublic personal financial information does not include:*

(a) Health information;

(b) Publicly available information, except as included on a list described in subsection (1)(b) of this subsection R; or

(c) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.

(3) *Examples of lists.*

(a) Nonpublic personal financial information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information that is not publicly available, such as account numbers.

(b) Nonpublic personal financial information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived in whole or in part using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

S. “*Nonpublic personal health information*” means health information:

- (1) That identifies an individual who is the subject of the information; or
- (2) With respect to which there is a reasonable basis to believe that the information could be used to identify an individual.

T. (1) “*Personally identifiable financial information*” means any information:

- (a) A consumer provides to a financial institution to obtain a financial product or service from the financial institution;
- (b) About a consumer resulting from any transaction involving a financial product or service between a financial institution and a consumer; or
- (c) The financial institution otherwise obtains about a consumer in connection with providing a financial product or service to that consumer.

(2) *Examples.*

(a) *Information included.* Personally identifiable financial information includes:

- (i) Information a consumer provides to a financial institution on an application to obtain a loan, credit card, or other financial product or service;
- (ii) Account balance information, payment history, overdraft history, and credit or debit card purchase information;
- (iii) The fact that an individual is or has been one of the financial institution's customers or has obtained a financial product or service from the financial institution;
- (iv) Any information about the financial institution's consumer if it is disclosed in a manner that indicates that the individual is or has been the financial institution's consumer;
- (v) Any information that a consumer provides to a financial institution or that the financial institution or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;
- (vi) Any information the financial institution collects through an Internet “cookie” (an information collecting device from a web server); and

(vii) Information from a consumer report.

(b) *Information not included.* Personally identifiable financial information does not include:

(i) Health information.

(ii) A list of names and addresses of customers of an entity that is not a financial institution; and

(iii) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

U. (1) “*Publicly available information*” means any information that a financial institution has a reasonable basis to believe is lawfully made available to the general public from:

(a) federal, state, or local government records;

(b) Widely distributed media; or

(c) Disclosures to the general public that are required to be made by federal, state, or local law.

(2) *Reasonable basis.* A financial institution has a reasonable basis to believe that information is lawfully made available to the general public if the financial institution has taken steps to determine:

(a) That the information is of the type that is available to the general public; and

(b) Whether an individual can direct that the information not be made available to the general public and, if so, that the financial institution's consumer has not done so.

(3) *Examples.*

(a) *Government records.* Publicly available information in government records includes information in government real estate records and security interest filings.

(b) *Widely distributed media.* Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper, or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(c) *Reasonable basis.*

(i) A financial institution has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the financial institution has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(ii) A financial institution has a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if the financial institution has located the telephone number in the telephone book or the consumer has informed the financial institution that the telephone number is not unlisted.

ARTICLE II. PRIVACY AND OPT IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 5. Initial Privacy Notice to Consumers Required

A. Initial notice requirement. A financial institution shall provide a clear and conspicuous notice that accurately reflects its privacy policies and practices with respect to nonpublic personal information to:

(1) *Customer.* An individual who becomes the financial institution's customer, not later than when the financial institution establishes a customer relationship, except as provided in subsection E of this section; and

(2) *Consumer.* A consumer, before the financial institution discloses any nonpublic personal information about the consumer to any nonaffiliated third party, if the financial institution makes a disclosure other than as authorized by Sections 15, 16 and 17.

B. When initial notice to a consumer is not required. A financial institution is not required to provide an initial notice to a consumer under subsection A(2) of this section if:

(1) the financial institution does not disclose any nonpublic personal information about the consumer to any nonaffiliated third party, other than as authorized by Sections 15, 16 and 17, and the financial institution does not have a customer relationship with the consumer; or

(2) a notice has been provided by an affiliate, as long as the notice clearly identifies all affiliates to whom the notice applies and is accurate with respect to the financial institution and the other affiliates.

C. When the financial institution establishes a customer relationship.

(1) *General rule.* A financial institution establishes a customer relationship at the time the financial institution and the consumer enter into a continuing relationship.

(2) *Special rule for loans.* A financial institution establishes a customer relationship with a consumer when the financial institution originates a loan to the consumer for personal, family, or household purposes. If the financial institution subsequently transfers the servicing

rights to that loan to another financial institution, the customer relationship transfers with the servicing rights.

(3) (a) *Examples of establishing customer relationship.* A financial institution establishes a customer relationship when the consumer:

- (i) Opens a credit card account with the financial institution;
- (ii) Executes the contract to open a deposit account with the financial institution, obtains credit from the financial institution, or purchases insurance from the financial institution;
- (iii) Agrees to obtain financial, economic, or investment advisory services from the financial institution for a fee; or
- (iv) Becomes the financial institution's client for the purpose of the financial institution's providing credit counseling or tax preparation services.

(b) *Examples of loan rule.* A financial institution establishes a customer relationship with a consumer who obtains a loan for personal, family, or household purposes when the financial institution:

- (i) Originates the loan to the consumer; or
- (ii) Purchases the servicing rights to the consumer's loan.

D. *Existing customers.* When an existing customer obtains a new financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes, the financial institution satisfies the initial notice requirements of subsection A of this section as follows:

- (1) The financial institution may provide a revised policy notice, under Section 9, that covers the customer's new financial product or service; or
- (2) If the initial, revised or annual notice that the financial institution most recently provided to that customer was accurate with respect to the new financial product or service, the financial institution does not need to provide a new privacy notice under subsection A of this section.

E. *Exceptions to allow subsequent delivery of notice.*

(1) A financial institution may provide the initial notice required by subsection A(1) of this section within a reasonable time after the financial institution establishes a customer relationship if:

- (a) Establishing the customer relationship is not at the customer's election; or

(b) Providing notice not later than when the financial institution establishes a customer relationship would substantially delay the customer's transaction and the customer agrees to receive the notice at a later time.

(2) *Examples.*

(a) *Not at customer's election.* Establishing a customer relationship is not at the customer's election if a financial institution acquires or is assigned a customer's deposit liability or the servicing rights to a customer's loan from another financial institution and the customer does not have a choice about the financial institution's acquisition.

(b) *Substantial delay of customer's transaction.* Providing notice not later than when a financial institution establishes a customer relationship would substantially delay the customer's transaction when:

(i) The financial institution and the individual agree over the telephone to enter into a customer relationship involving prompt delivery of the financial product or service; or

(ii) The financial institution establishes a customer relationship with an individual under a program authorized by Title IV of the Higher Education Act of 1965 (20 U.S.C. 1070 et seq.) or similar student loan programs where loan proceeds are disbursed promptly without prior communication between the financial institution and the customer.

(c) *No substantial delay of customer's transaction.* Providing notice not later than when a financial institution establishes a customer relationship would not substantially delay the customer's transaction when the relationship is initiated in person at the financial institution's office or through other means by which the customer may view the notice, such as on a web site.

F. *Delivery.* When a financial institution is required to deliver an initial privacy notice by this section, the financial institution shall deliver it according to Section 10. If the financial institution uses a short-form initial notice for non-customers according to Section 7D, the financial institution may deliver its privacy notice according to Section 7D(3).

Section 6. Annual Privacy Notice to Customers Required

A. (1) *General rule.* Except as provided in subsection E of this section, a financial institution shall provide a clear and conspicuous notice to customers that accurately reflects its privacy policies and practices with respect to nonpublic personal information not less than annually during the continuation of the customer relationship. Annually means at least once in any period of twelve (12) consecutive months during which that relationship exists. A financial institution may define the twelve-consecutive-month period, but the financial institution shall apply it to the customer on a consistent basis.

(2) *Example.* A financial institution provides a notice annually if it defines the twelve-consecutive-month period as a calendar year and provides the annual notice to the customer once in each calendar year following the calendar year in which the financial institution provided the initial notice. For example, if a customer opens an account on any day of year 1, the financial institution shall provide an annual notice to that customer by December 31 of year 2.

B. (1) *Termination of customer relationship.* A financial institution is not required to provide an annual notice to a former customer. A former customer is an individual with whom a financial institution no longer has a continuing relationship.

(2) *Examples.* A financial institution's customer becomes a former customer:

(a) In the case of a deposit account, when the account is inactive under the financial institution's policies;

(b) In the case of a closed-end loan, when the customer pays the loan in full, the financial institution charges off the loan, or the financial institution sells the loan without retaining servicing rights;

(c) In the case of a credit card relationship or other open-end credit relationship, when the financial institution no longer provides any statements or notices to the customer concerning that relationship or the financial institution sells the credit card receivables without retaining servicing rights;

(d) When the financial institution has not communicated with the customer about the relationship for a period of 12 consecutive months, other than to provide annual privacy notices or promotional material;

(e) If the individual's last known address according to the financial institution's records is invalid. An address of record is invalid, for purposes of this rule, if mail sent to that address by the financial institution has been returned by the postal authorities as undeliverable and if subsequent attempts by the financial institution to obtain a current valid address for the individual have been unsuccessful; or

(f) At the time the customer completes execution of all documents related to the real estate closing, payment for those services has been received, or the financial institution has completed all of its responsibilities with respect to the settlement, including filing documents on the public record, whichever is later.

C. *Special rule for loans.* If a financial institution does not have a customer relationship with a consumer under the special rule for loans in subsection C(2) of Section 5, then the financial institution need not provide an annual notice to that consumer under this section.

D. *Delivery*. When a financial institution is required by this section to deliver an annual privacy notice, the financial institution shall deliver it according to Section 10.

E. *Exception to annual privacy notice requirement*.

(1) *When exception available*. A financial institution is not required to deliver an annual privacy notice if:

(a) The financial institution provides nonpublic personal information to nonaffiliated third parties only in accordance with the provisions of Sections 14, 15, and 16 of this regulation;

(b) The financial institution does not disclose information to or among its affiliates in a manner that would require an opt-in under the Vermont Fair Credit Reporting Act, 9 V.S.A. §2480e;

(c) Any disclosures the financial institution is required to make under Section 624 of the federal Fair Credit Reporting Act (15 U.S.C. § 1681s-3) and the federal implementing regulations (as modified by 15 U.S.C. § 1681t (b)(2) and the Vermont Fair Credit Reporting Act, if applicable) have been satisfied previously or the annual privacy notice is not the only notice provided to satisfy the requirement in this subsection (c);

(d) The financial institution has not changed its policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed to the customer in the most recent privacy notice (whether initial, annual, or revised) provided pursuant to this regulation; and

(e) The financial institution posts its current privacy notice continuously and in a clear and conspicuous manner on a page of its web site on which the only content is the privacy notice, without requiring the customer to provide any information such as a login name or password or agree to any conditions to access the page.

(2) *Delivery of annual privacy notice after financial institution no longer meets requirements for exception*. If a financial institution has been excepted from delivering an annual privacy notice pursuant to subsection E(1) of this section and changes its policies or practices in such a way that it no longer meets the requirements for the exception, the financial institution must provide a new privacy notice to customers at least 60 days prior to the effective date of the change in its policies or practices. The new privacy notice will be treated as an initial privacy notice for purposes of this regulation and the financial institution's obligation to provide an annual privacy notice thereafter shall be determined in accordance with the requirements and exceptions of this section.

Section 7. Information to be Included in Privacy Notices

A. *General rule*. The initial, annual and revised privacy notices that a financial institution provides under Sections 5, 6 and 9 shall include each of the following items of information, in

addition to any other information the financial institution wishes to provide, that applies to the financial institution and to the consumers to whom the financial institution sends its privacy notice:

- (1) The categories of nonpublic personal information that the financial institution collects;
- (2) The categories of nonpublic personal information that the financial institution discloses;
- (3) The categories of affiliates and nonaffiliated third parties to whom the financial institution discloses nonpublic personal information, other than those parties to whom the financial institution discloses information under Sections 15, 16 and 17;
- (4) The categories of nonpublic personal information about the financial institution's former customers that the financial institution discloses and the categories of affiliates and nonaffiliated third parties to whom the financial institution discloses nonpublic personal information about the financial institution's former customers, other than those parties to whom the financial institution discloses information under Sections 15, 16 and 17;
- (5) If a financial institution discloses nonpublic personal information to a nonaffiliated third party under Section 14 (and no other exception in Sections 15 and 16 applies to that disclosure), a separate description of the categories of information that the financial institution discloses as modified by Section 14 of this regulation and the categories of nonaffiliated third parties with whom the financial institution has contracted;
- (6) An explanation of the consumer's right to opt in under Section 11A prior to the disclosure of nonpublic personal financial information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at any time;
- (7) Any disclosures that the financial institution makes under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. § 1681a(d)(2)(A)(iii)) and the federal implementing regulations, as modified by 15 U.S.C. § 1681t (b)(2) and the Vermont Fair Credit Reporting Act, 9 V.S.A. § 2480e (that is, under Vermont law, require that consumers consent prior to disclosures of information among affiliates);
- (8) The financial institution's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and
- (9) Any disclosure that the financial institution makes under subsection B of this section.

B. Description of parties subject to exceptions. If a financial institution discloses nonpublic personal information as authorized under Sections 15, 16 and 17, the financial institution is not required to list those exceptions in the initial or annual privacy notices required by Sections 5 and 6. When describing the categories of parties to whom disclosure is made, the financial institution is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.

C. Examples.

(1) *Categories of nonpublic personal information that the financial institution collects.* A financial institution satisfies the requirement to categorize the nonpublic personal information it collects if the financial institution categorizes it according to the source of the information, as applicable:

- (a) Information from the consumer;
- (b) Information about the consumer's transactions with the financial institution or its affiliates;
- (c) Information about the consumer's transactions with nonaffiliated third parties; and
- (d) Information from a consumer reporting agency.

(2) *Categories of nonpublic personal financial information a financial institution discloses.*

(a) A financial institution satisfies the requirement to categorize nonpublic personal information it discloses if the financial institution categorizes the information according to source, as described in subdivision (1) of this subsection C, as applicable, and provides a few examples to illustrate the types of information in each category. These might include:

- (i) Information from the consumer, including application information, such as assets and income and identifying information, such as name, address and social security number;
 - (ii) Transaction information, such as information about balances, payment history and parties to the transaction; and
 - (iii) Information from consumer reports, such as a consumer's creditworthiness and credit history.
- (b) A financial institution does not adequately categorize the information that it discloses if the financial institution uses only general terms, such as transaction information about the consumer.
- (c) If a financial institution reserves the right to disclose all of the nonpublic personal financial information about consumers that it collects, the financial institution may simply state that fact without describing the categories or examples of nonpublic personal financial information that the financial institution discloses.

(3) *Categories of affiliates and nonaffiliated third parties to whom the financial institution discloses.*

(a) A financial institution satisfies the requirement to categorize the affiliates and nonaffiliated third parties to which the financial institution discloses nonpublic personal information about consumers if the financial institution lists the following categories, as applicable, and a few examples to illustrate the types of third parties in each category.

- (i) Financial service providers;
- (ii) Non-financial companies; and
- (iii) Others.

(b) A financial institution also may categorize the affiliates and nonaffiliated third parties to which it discloses nonpublic personal information about consumers using more detailed categories.

(4) *Disclosures under exception for service providers and joint marketers.* If a financial institution discloses nonpublic personal financial information under the exception in Section 14 to a nonaffiliated third party to market products or services that it offers alone or jointly with another financial institution, the financial institution satisfies the disclosure requirement of Subsection A(5) of this section if it:

(a) Subject to the limitations in Section 14, lists the categories of nonpublic personal financial information it discloses, using the same categories and examples the financial institution used to meet the requirements of Subsection A(2) of this section, as applicable; and

(b) States whether the third party is:

- (i) A service provider that performs marketing services on the financial institution's behalf or on behalf of the financial institution and another financial institution; or
- (ii) A financial institution with whom the financial institution has a joint marketing agreement.

(5) *Simplified notices.* If a financial institution does not disclose, and does not wish to reserve the right to disclose, nonpublic personal information about customers or former customers to affiliates or nonaffiliated third parties except as authorized under Sections 15, 16 and 17, the financial institution may simply state that fact, in addition to the information it must provide under subsections A(1), A(8), A(9), and subsection B of this section.

(6) *Confidentiality and security.* A financial institution describes its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information if it does both of the following:

- (a) Describes in general terms who is authorized to have access to the information; and

(b) States whether the financial institution has security practices and procedures in place to ensure the confidentiality of the information in accordance with the financial institution's policy. The financial institution is not required to describe technical information about the safeguards it uses.

D. Short-form initial notice with opt in notice for non-customers.

(1) A financial institution may satisfy the initial notice requirements in Sections 5A (2) and 8C for a consumer who is not a customer by providing a short-form initial notice at the same time as the financial institution delivers an opt in notice under Section 8.

(2) A short-form initial notice shall:

(a) Be clear and conspicuous;

(b) State that the financial institution's privacy notice is available upon request; and

(c) Explain a reasonable means by which the consumer may obtain that notice.

(3) The financial institution shall deliver its short-form initial notice according to Section 10. The financial institution is not required to deliver its privacy notice with its short-form initial notice. The financial institution instead may simply provide the consumer a reasonable means to obtain its privacy notice. If a consumer who receives the financial institution's short-form notice requests the financial institution's privacy notice, the financial institution shall deliver its privacy notice according to Section 10.

(4) *Examples of obtaining privacy notice.* The financial institution provides a reasonable means by which a consumer may obtain a copy of its privacy notice if the financial institution:

(a) Provides a toll-free telephone number that the consumer may call to request the notice; or

(b) For a consumer who conducts business in person at the financial institution's office, maintains copies of the notice on hand that the financial institution provides to the consumer immediately upon request.

E. Future disclosures. The financial institution's notice may include:

(1) Categories of nonpublic personal financial information that the financial institution reserves the right to disclose in the future, but does not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom the financial institution reserves the right in the future to disclose, but to whom the financial institution does not currently disclose, nonpublic personal financial information.

F. *Sample clauses.* Sample clauses illustrating some of the notice content required by this section are included in Appendix A of this regulation.

G. *Federal Model Privacy Form.*

(1) Vermont statutes and regulations relating to consumer privacy contain privacy notice content requirements with significant differences from federal content requirements. Among other differences, Vermont is an “opt-in” state.

(2) Federal Regulation P (Privacy of Consumer Financial Information), 12 C.F.R. Part 1016, contains a model privacy form at Appendix to Part 1016 – Model Privacy Form (“Federal Model Privacy Form”).

(3) A financial institution that uses the Federal Model Privacy Form in accordance with the instructions for use of the Model Federal Privacy Form as set forth in the Appendix to Part 1016, as supplemented by the requirements of this subsection, is in compliance with the content notice requirements of this Regulation. Use of the Federal Model Privacy Form is not required. Financial institutions may use other types of privacy notices so long as the notices comply with this Regulation.

(4) Vermont laws and regulations require financial institutions to obtain an “opt-in” consent from a consumer prior to sharing nonpublic personal information with an affiliate or with a nonaffiliated third party, except as otherwise specifically permitted by this regulation. A financial institution may use the Federal Model Privacy Form to comply with this regulation in either of the following ways:

Option 1. A financial institution may provide a generalized notice to its Vermont consumers that answers “no” to each of the questions about whether it shares information: (i) “For our affiliates’ everyday business purposes – information about your creditworthiness;” **and** (ii) “for nonaffiliates to market to you;” **OR**

Option 2. A financial institution can provide a generalized notice to consumers across a number of states, including Vermont, and answer “yes” to the questions in Option 1 above, **provided** it includes a discussion on the application of Vermont law in the “Other Important Information” box on page 2 of the Federal Model Privacy Form **and** complies with the requirements in subsection 5 below.

(5) A financial institution that chooses to use the Federal Model Privacy Form as provided in Option 2 above shall provide the following information:

(a) The “Other Important Information” box on the Federal Model Privacy Form contains statements that convey the following information:

Other Important Information

For Vermont Members/Customers.

- We will not disclose information about your creditworthiness to our affiliates and will not disclose your personal information, financial information, credit report, or health information to nonaffiliated third parties to market to you, other than as permitted by Vermont law, unless you authorize us to make those disclosures.
- Additional information concerning our privacy policies can be found at [website link] or call [telephone number].

AND

(b) The additional information provided on the financial institution's website contains the information required by this regulation; to the extent such information is not already included in the financial institution's privacy notice.

Section 8. Form of Opt in Notice to Consumers and Opt in Methods

A. (1) *Form of opt in notice.* A financial institution required to provide an opt in notice under Section 11A may not disclose any nonpublic personal financial information pertaining to a consumer to a nonaffiliated third party unless the financial institution:

- (a) Has provided to the consumer a clear and conspicuous notice, in writing or electronic form, of the categories of nonpublic personal financial information that may be disclosed and the categories of nonaffiliated third parties to whom the financial institution discloses nonpublic personal financial information.
- (b) Has identified the financial products or services that the consumer obtains from the financial institution, either singly or jointly, to which the opt in direction would apply;
- (c) Has identified the methods by which the consumer may subsequently revoke the opt in direction;
- (d) Has clearly and conspicuously requested in writing or in electronic form that the consumer affirmatively authorize such disclosure; and
- (e) Has obtained from the consumer such affirmative consent and such consent has not been withdrawn.

(2) *Unreasonable revocation of opt in direction.* A means of revocation of an opt in direction is unreasonable if the only means is for the consumer to write his or her own letter or is to use a check-off box that was provided with the initial notice but is not included with subsequent notices.

(3) *Duration and withdrawal of consent.* A consumer's direction to opt in under this subsection is effective until the consumer revokes it in writing or, if the consumer agrees, electronically; further provided however, any withdrawal or revocation of consent is subject to the rights of any financial institution that acted reasonably in reliance on the consent prior to knowledge of its withdrawal or revocation. When a customer relationship terminates, the customer's opt in direction continues to apply to the nonpublic personal financial information collected during or related to that relationship. If the individual subsequently establishes a new customer relationship with the financial institution, the opt in direction that applied to the former relationship does not apply to the new relationship.

(4) A financial institution may not disclose any aggregate list of consumers containing or derived from nonpublic personal financial information to a nonaffiliated third party unless the financial institution has satisfied, for each consumer on the list, the requirements of subdivisions (a), (b), (c), (d) and (e) of subsection A (1) of this section.

(5) This section shall not restrict a financial institution from disclosing nonpublic personal information as authorized in Sections 14, 15, 16 or 17.

(6) A financial institution shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal financial information.

(7) *Joint relationships.* If two or more consumers jointly obtain a financial product or service from a financial institution, the financial institution may only disclose nonpublic personal financial information of a consumer to a nonaffiliated third party after obtaining an affirmative consent notice from that consumer. Joint information may only be disclosed after obtaining the affirmative consent notice from all joint consumers of the financial product or service.

B. *Same form as initial notice permitted.* A financial institution may provide the opt in notice required by this section together with or on the same written or electronic form as the initial notice the financial institution provides in accordance with Section 5.

C. *Initial notice required when opt in notice under this section delivered subsequent to initial notice.* If a financial institution provides the opt in notice later than required for the initial notice in accordance with Section 5, the financial institution shall also include a copy of the initial notice with the opt in notice in writing or, if the consumer agrees, electronically.

D. *Delivery.* When a financial institution is required to deliver an opt in notice by this section, the financial institution shall deliver it according to Section 10.

Section 9. Revised Privacy Notices

A. *General rule.* Except as otherwise authorized in this regulation, a financial institution shall not, directly or through an affiliate, disclose any nonpublic personal information about a consumer to any nonaffiliated third party other than as described in the initial notice that the financial institution provided to that consumer under Section 5, unless:

- (1) The financial institution has provided to the consumer a clear and conspicuous revised notice that accurately describes its policies and practices;
- (2) The financial institution has provided to the consumer a new opt in notice; and
- (3) The consumer has provided affirmative consent to the disclosure described in the notice.

B. *Examples.*

- (1) Except as otherwise permitted by Sections 14, 15 and 16, a financial institution shall provide a revised notice before it:
 - (a) Discloses a new category of nonpublic personal financial information to any nonaffiliated third party;
 - (b) Discloses nonpublic personal financial information to a new category of nonaffiliated third party; or
 - (c) Discloses nonpublic personal financial information about a former customer to a nonaffiliated third party, if that former customer has not given affirmative consent regarding that disclosure.
- (2) A revised notice is not required if the financial institution discloses nonpublic personal financial information to a new nonaffiliated third party that the financial institution adequately described in its prior notice.

C. *Delivery.* When a financial institution is required to deliver a revised privacy notice by this section, the financial institution shall deliver it according to Section 10.

D. Nothing in this regulation shall relieve any financial institution of any requirement under the federal or Vermont Fair Credit Reporting Acts or regulations promulgated thereunder with respect to notice and consumer consent for disclosures to affiliates.

Section 10. Delivery

A. *How to provide notices.* A financial institution shall provide any notices that this regulation requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer agrees, electronically.

B. (1) *Examples of reasonable expectation of actual notice.* A financial institution may reasonably expect that a consumer will receive actual notice if the financial institution:

- (a) Hand-delivers a printed copy of the notice to the consumer;
- (b) Mails a printed copy of the notice to the last known address of the consumer;

(c) For a consumer who conducts transactions electronically, posts the notice on the electronic site and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular financial product or service; or

(d) For an isolated transaction with a consumer, such as an ATM transaction, posts the notice on the ATM screen and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular financial product or service.

(2) *Examples of unreasonable expectation of actual notice.* A financial institution may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:

(a) Only posts a sign in its branch or office or generally publishes advertisements of its privacy policies and practices; or

(b) Sends the notice via electronic mail to a consumer who does not obtain a financial product or service from the financial institution electronically.

C. Annual notices only - Reasonable Expectation. A financial institution may reasonably expect that a customer will receive actual notice of the financial institution's annual privacy notice if:

(1) The customer uses the financial institution's web site to access financial products and services electronically and agrees to receive notices at the web site and the financial institution posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or

(2) The customer has requested that the financial institution refrain from sending any information regarding the customer relationship, and the financial institution's current privacy notice remains available to the customer upon request.

D. Oral description of notice insufficient. A financial institution may not provide any notice required by this regulation solely by orally explaining the notice, either in person or over the telephone.

E. Retention or accessibility of notices for customers.

(1) For customers only, a financial institution shall provide the initial notice required by Section 5A(1), the annual notice required by Section 6A, and the revised notice required by Section 9 so that the customer can retain them or obtain them later in writing or, if the customer agrees to electronic receipt, transmit them in a form that the customer can download and print.

(2) *Examples of retention or accessibility.* A financial institution provides a privacy notice to the customer so that the customer can retain it or obtain it later if the financial institution:

- (a) Hand-delivers a printed copy of the notice to the customer;
- (b) Mails a printed copy of the notice to the last known address of the customer; or
- (c) Makes its current privacy notice available on a web site (or a link to another web site) for the customer who obtains a financial product or service electronically and agrees to receive the notice at the web site. Electronic receipt must include the ability to download and print the notice.

F. *Joint notice with other financial institutions.* A financial institution may provide a joint notice from the financial institution and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the financial institution and the other institutions. A financial institution also may provide a notice on behalf of another financial institution.

G. *Joint relationships.* If two (2) or more consumers jointly obtain a financial product or service from a financial institution, the financial institution may satisfy the initial, annual and revised notice requirements of Sections 5A, 6A and 9A, respectively, by providing one notice to those consumers jointly.

ARTICLE III. LIMITS ON DISCLOSURES OF FINANCIAL INFORMATION

Section 11. Limits on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties

A. (1) *Conditions for disclosure.* Except as otherwise authorized in this regulation, a financial institution may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party unless:

- (a) The financial institution has provided to the consumer an initial notice as required under Section 5;
- (b) The financial institution has provided to the consumer an opt in notice under Section 8 of this regulation; and
- (c) The consumer has authorized the disclosure in writing or, if the consumer agrees, electronically.

(2) *Opt in definition.* “Opt in” means the written or, if the consumer agrees, electronic authorization of the consumer allowing a financial institution to disclose nonpublic personal financial information to a nonaffiliated third party, other than as permitted under Sections 14, 15 or 16 of this regulation.

B. *Application of opt in to all consumers and all nonpublic personal financial information.*

(1) A financial institution shall comply with this section, regardless of whether the financial institution and the consumer have established a customer relationship.

(2) Unless a financial institution complies with this section, the financial institution may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer that the financial institution has collected, regardless of whether the financial institution collected it before or after providing the opt in notice.

C. Partial opt in. A financial institution may allow a consumer to select certain nonpublic personal financial information or certain nonaffiliated third parties with respect to which the consumer wishes to opt in.

Section 12. Limits on Redisclosure and Reuse of Nonpublic Personal Financial Information

A. (1) Information the financial institution receives under an exception. If a financial institution receives nonpublic personal financial information from a nonaffiliated financial institution under an exception in Sections 15 or 16 of this regulation, the financial institution's disclosure and use of that information is limited as follows:

(a) The financial institution may disclose the information to the affiliates of the nonaffiliated financial institution from which the financial institution received the information;

(b) The financial institution may disclose the information to its affiliates, but the financial institution's affiliates may, in turn, disclose and use the information only to the extent that the financial institution may disclose and use the information; and

(c) The financial institution may disclose and use the information pursuant to an exception in Sections 15 or 16 of this regulation, in the ordinary course of business to carry out the activity covered by the exception under which the financial institution received the information.

(2) *Example.* If a financial institution receives a customer list from a nonaffiliated financial institution in order to provide account processing services under the exception in Section 15, the financial institution may disclose that information under any exception in Sections 15 and 16 in the ordinary course of business in order to provide those services. For example, the financial institution could disclose the information in response to a properly authorized subpoena or to its attorneys, accountants, and auditors. The financial institution could not disclose that information to a third party for marketing purposes or use that information for its own marketing purposes.

B. (1) Information a financial institution receives outside of an exception. If a financial institution receives nonpublic personal financial information from a nonaffiliated financial institution other than under an exception in Sections 15 or 16 of this regulation, the financial institution may disclose the information only:

- (a) To the affiliates of the nonaffiliated financial institution from which the financial institution received the information;
- (b) To its affiliates, but its affiliates may, in turn, disclose the information only to the extent that the financial institution may disclose the information; and
- (c) To any other person, if the disclosure would be lawful if made directly to that person by the nonaffiliated financial institution from which the financial institution received the information.

(2) *Example.* If a financial institution obtains a customer list from a nonaffiliated financial institution outside of the exceptions in Sections 15 or 16:

- (a) The financial institution may use that list for its own purposes; and
- (b) The financial institution may disclose that list to another nonaffiliated third party only if the nonaffiliated financial institution from which the financial institution purchased the list could have lawfully disclosed the list to that third party. That is, the financial institution may disclose the list in accordance with the privacy policy of the nonaffiliated financial institution from which the financial institution received the list, as limited by the absence or limitation of any opt in direction of each consumer whose nonpublic personal financial information the financial institution intends to disclose, and the financial institution may disclose the list in accordance with an exception in Sections 15 or 16, such as to the financial institution's attorneys or accountants.

C. Information a financial institution discloses under an exception. If a financial institution discloses nonpublic personal financial information to a nonaffiliated third party under an exception in Sections 15 or 16 of this regulation, the third party may disclose and use that information only as follows:

- (1) The third party may disclose the information to the financial institution's affiliates;
- (2) The third party may disclose the information to its affiliates, but its affiliates may, in turn, disclose and use the information only to the extent that the third party may disclose and use the information; and
- (3) The third party may disclose and use the information pursuant to an exception in Sections 15 or 16 in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

D. Information a financial institution discloses outside of an exception. If a financial institution discloses nonpublic personal financial information to a nonaffiliated third party other than under an exception in Sections 15 or 16 of this regulation, the third party may disclose the information only:

- (1) To the financial institution's affiliates;

(2) To the third party's affiliates, but the third party's affiliates, in turn, may disclose the information only to the extent the third party can disclose the information; and

(3) To any other person, if the disclosure would be lawful if the financial institution made it directly to that person.

E. Nothing in this regulation shall authorize any financial institution to make any disclosure to an affiliate not otherwise in compliance with any requirement of the federal Fair Credit Reporting Act or regulations promulgated thereunder or the Vermont Fair Credit Reporting Act, including, but not limited to, notice and consumer consent.

Section 13. Limits on Sharing Account Number Information for Marketing Purposes

A. General prohibition on disclosure of account numbers. A financial institution shall not, directly or through an affiliate, disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a consumer's transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer. A financial institution shall not provide an account number or similar form of access number or code in an encrypted form to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

B. Exceptions. Subsection A of this section does not apply if a financial institution discloses an account number or similar form of access number or access code:

(1) To the financial institution's agent or service provider solely in order to perform marketing for the financial institution's own products or services, as long as the service provider is not authorized to directly initiate charges to the account; or,

(2) To a participant in a private label credit card or affinity or similar program where the participants in the program are identified to the customer when the customer enters into the program.

C. Examples.

(1) *Account number.* An account number, or similar form of access number or access code, shall include a number or code in an encrypted form.

(2) *Transaction account.* A transaction account is an account other than a deposit account or a credit card account. An account is not a transaction account if a third party cannot initiate charges to it.

ARTICLE IV. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 14. Exception to Opt In Requirements for Disclosure of Nonpublic Personal Information for Service Providers and Joint Marketing

A. General rule.

(1) The opt in requirements in Sections 8 and 11 do not apply when a financial institution provides nonpublic personal information to a nonaffiliated third party to perform services for the financial institution or functions on the financial institution's behalf, if the financial institution:

(a) Provides the initial notice in accordance with Section 5;

(b) Enters into a contractual agreement with the third party that prohibits the nonaffiliated third party from disclosing or using the information other than to carry out the purposes for which the financial institution disclosed the information, including use under an exception in Sections 15 or 16 in the ordinary course of business to carry out those purposes; and,

(c) For joint agreements for marketing,

(i) provides only the consumer's name, contact information and own transaction and experience information within the meaning of the federal Fair Credit Reporting Act, 15 U.S.C. § 1681a (d)(2)(A)(i) and the Vermont Fair Credit Reporting Act, 9 V.S.A. § 2480a (2)(A); and,

(ii) in the event health information is provided as own transaction and experience information as defined in subdivision (i) of this subsection (c), complies with Section 20 of this regulation.

(2) Examples.

(a) If a financial institution discloses nonpublic personal information under this section to a financial institution with which the financial institution performs joint marketing, the financial institution's contractual agreement with that institution meets the requirements of subdivisions (1)(b) of subsection A of this section if it prohibits the institution from disclosing or using the nonpublic personal information except as necessary to carry out the joint marketing or under an exception in Sections 15 or 16 in the ordinary course of business to carry out that joint marketing.

(b) A financial institution that complies with the provisions of Section 14.A (1) (a) and (b) may provide nonpublic personal information to a service provider that is a nonaffiliated third party agent of that financial institution (e.g. a mailing service that is an independent contractor as to the financial institution) to enable the agent to print, label and mail a solicitation for the financial institution's product on behalf of the financial

institution. Such disclosure shall not be subject to the limitations of subsection A (1)(c) of this section.

B. *Service may include joint marketing.* The services a nonaffiliated third party performs for a financial institution under subsection A of this section may include marketing of the financial institution's own products or services or marketing of financial products or services offered pursuant to joint agreements between the financial institution and one or more financial institutions.

C. *Definition of "joint agreement."* "Joint agreement" means a written contract pursuant to which a financial institution and one or more financial institutions jointly offer, endorse or sponsor a financial product or service.

Section 15. Exceptions to Notice and Opt In Requirements for Disclosure of Nonpublic Personal Financial Information for Processing and Servicing Transactions

A. *Exceptions for processing transactions at consumer's request.* The requirements for initial notice in Section 5A(2), the opt in requirements in Sections 8 and 11, and service providers and joint marketing in Section 14 do not apply if the financial institution discloses nonpublic personal financial information as necessary to effect, administer or enforce a transaction that a consumer requests or authorizes, or in connection with:

- (1) Servicing or processing a financial product or service that a consumer requests or authorizes;
- (2) Maintaining or servicing the consumer's account with a financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or
- (3) A proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer.

B. *"Necessary to effect, administer or enforce a transaction"* means that the disclosure is:

- (1) Required, or is one of the lawful or appropriate methods, to enforce the financial institution's rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or
- (2) Required, or is a usual, appropriate or acceptable method:
 - (a) To carry out the transaction or the product or service business of which the transaction is a part, and record, service or maintain the consumer's account in the ordinary course of providing the financial product or service;
 - (b) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

- (c) To provide a confirmation, statement or other record of the transaction, or information on the status or value of the financial product or service to the consumer or the consumer's agent or broker;
- (d) To accrue or recognize incentives or bonuses associated with the transaction that are provided by a financial institution or any other party;
- (e) To the extent permitted under applicable law, to underwrite insurance at the consumer's request or for reinsurance purposes, or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects or as otherwise required or specifically permitted by federal or state law; or
- (f) In connection with:
 - (i) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited or otherwise paid using a debit, credit or other payment card, check or account number, or by other payment means;
 - (ii) The transfer of receivables, accounts or interests therein; or
 - (iii) The audit of debit, credit or other payment information.

Section 16. Other Exceptions to Notice and Opt In Requirements for Disclosure of Nonpublic Personal Financial Information

A. Exceptions to opt in requirements. The requirements for initial notice to consumers in Section 5A(2), the opt in requirements in Sections 8 and 11, and service providers and joint marketing in Section 14 do not apply when a financial institution discloses nonpublic personal financial information:

- (1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;
- (2) (a) To protect the confidentiality or security of a financial institution's records pertaining to the consumer, service, product or transaction;
- (b) To protect against or prevent actual or potential fraud or unauthorized transactions, claims or other liability;
- (c) For required institutional risk control or for resolving consumer disputes or inquiries;
- (d) To persons holding a legal or beneficial interest relating to the consumer; or

- (e) To persons acting in a fiduciary or representative capacity on behalf of the consumer;
- (3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating a financial institution, persons that are assessing the financial institution's compliance with industry standards, and the financial institution's attorneys, accountants and auditors;
- (4) To the extent specifically permitted or required under other provisions of law and in accordance with the federal Right to Financial Privacy Act of 1978 (12 U.S.C. § 3401 et seq.), to law enforcement agencies (including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, the Securities and Exchange Commission, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping) and the Federal Trade Commission), to state and federal civil and administrative authorities (including, but not limited to, a state insurance authority, a state banking authority and a state securities authority), selfregulatory organizations or for an investigation on a matter related to public safety;
- (5) (a) To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.); or
 - (b) From a consumer report reported by a consumer reporting agency;
- (6) In connection with a proposed or actual affiliation, reorganization, sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal financial information concerns solely consumers of the business or unit;
- (7) (a) To comply with federal, state or local laws, rules and other applicable legal requirements;
 - (b) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities;
 - (c) To respond to judicial process or government regulatory authorities having jurisdiction over a financial institution for examination, compliance or other purposes as authorized by law; or
- (8) As otherwise permitted under subchapter 2 of chapter 200 of title 8 V.S.A.

B. Examples of consent and revocation of consent.

- (1) A consumer may specifically consent to the disclosure to a nonaffiliated insurance company of the fact that the consumer has applied to the financial institution for a mortgage so that the insurance company can offer homeowner's insurance to the consumer.

(2) A consumer may revoke any authorization given to a financial institution at any time, subject to the rights of any person that acted in reliance on the authorization prior to notice of the revocation.

ARTICLE V. RULES FOR HEALTH INFORMATION

Section 17. When Authorization Required for Disclosure of Nonpublic Personal Health Information

A. *General rule.* A financial institution shall not disclose nonpublic personal health information about a consumer or customer unless an authorization is obtained from the consumer or customer whose nonpublic personal health information is sought to be disclosed.

B. *Exceptions.* Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a financial institution for the following:

(1) any activity that would permit disclosure without opt in by the consumer or customer pursuant to Section 15 or 16 of this regulation if the information were nonpublic personal financial information;

(2) in connection with the conduct by the financial institution directly of the business of insurance, any activity that would permit disclosure without authorization pursuant to Section 17.B or 17.C of Insurance Regulation IH-2001-01 (Privacy of Consumer Financial and Health Information Regulation);

(3) any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services, except as provided in Section 20 of this regulation; and

(4) any activity required pursuant to governmental reporting authority or to comply with legal process.

C. Additional categories of disclosures may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of activities that are financial in nature or incidental to such financial activities as described in the Section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. § 1843 (k)) and are fair and reasonable to the interest of consumers.

Section 18. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article V shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer or customer who is the subject of the nonpublic personal health information;

(2) A general description of the types of nonpublic personal health information to be disclosed;

(3) General descriptions of the parties to whom the financial institution discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

(4) The signature of the consumer or customer who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer or customer may revoke the authorization at any time and the procedure for making a revocation.

B. An authorization for the purposes of this Article V shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer or customer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article V at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

D. A financial institution shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

Section 19. Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer or a customer as part of an opt in notice pursuant to Section 10, provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer or customer unless the financial institution intends to disclose protected health information pursuant to Section 17A.

Section 20. Relationship to Federal Rules

Nothing in this regulation modifies, limits, or supersedes the standards and provisions of 45 C.F.R. Parts 160 and 164 governing individually identifiable health information promulgated by the Secretary of Health and Human Services under the authority of sections 262 and 264 of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. §§1320d - 1320d-8), provided, however, that persons subject to this regulation are prohibited from making disclosures under the provisions of 45 C.F.R. § 164.514 (e)(2) of those rules, without the consumer's prior written consent. Nothing in this regulation shall be deemed to make applicable any provision of the federal Health Insurance Portability and Accountability Act of 1996 or the regulations promulgated thereunder to any financial institution not otherwise subject thereto.

Section 21. Relationship to State Laws

Nothing in this regulation shall preempt or supersede existing state law related to medical records, health or insurance information privacy.

ARTICLE VI. ADDITIONAL PROVISIONS

Section 22. Protection and Application of Fair Credit Reporting Acts

A. No inference shall be drawn on the basis of the provisions of this regulation regarding whether information is transaction or experience information under Section 603 of the federal Fair Credit Reporting Act.

B. Nothing in this regulation shall be construed to modify, limit or supersede the operation of the Vermont Fair Credit Reporting Act (9 V.S.A. §§ 2480a - 2480g). No inference shall be drawn on the basis of the provisions of this regulation regarding whether information is transaction or experience information under Section 2480a (2) of the Vermont Fair Credit Reporting Act. This regulation shall not be construed to extend the application of the Vermont Fair Credit Reporting Act to persons who are not residents of Vermont.

Section 23. Nondiscrimination

A. A financial institution shall not unfairly discriminate against a consumer or customer because that consumer or customer has not opted in to the disclosure of his or her nonpublic personal financial information pursuant to the provisions of this regulation.

B. A financial institution shall not unfairly discriminate against a consumer or customer because that consumer or customer has not authorized the disclosure of his or her nonpublic personal health information pursuant to the provisions of this regulation.

Section 24. Violations

In addition to any other sanctions available to the commissioner under Vermont law for violations of this regulation, violations of this regulation are subject to the provisions of 8 V.S.A. §§ 10205 and 11601.

Section 25. Severability

If any section or portion of a section of this regulation or its applicability to any person or circumstance is held invalid by a court, the remainder of the regulation or the applicability of the provision to other persons or circumstances shall not be affected.

Section 26. Effective Date

This regulation is effective March 15, 2018.

APPENDIX A – SAMPLE CLAUSES

Financial institutions, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act and Vermont Fair Credit Reporting Act, such as a requirement to permit a consumer to opt in to disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A-1–Categories of information a financial institution collects (all institutions)

A financial institution may use this clause, as applicable, to meet the requirement of Section 7A(1) to describe the categories of nonpublic personal information the financial institution collects.

Sample Clause A-1:

We collect nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other forms;
- Information about your transactions with us, our affiliates or others; and
- Information we receive from a consumer reporting agency.

A-2–Categories of information a financial institution discloses (institutions that disclose outside of the exceptions)

A financial institution may use one of these clauses, as applicable, to meet the requirement of Section 7A(2) to describe the categories of nonpublic personal financial information the financial institution discloses. The financial institution may use these clauses if it discloses nonpublic personal financial information other than as permitted by the exceptions in Sections 14, 15 and 16.

Sample Clause A-2, Alternative 1:

We may disclose the following kinds of nonpublic personal financial information about you:

- Information we receive from you on applications or other forms, such as [provide illustrative examples, such as “your name, address, social security number, assets and income”];
- Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as “your account balance, payment history, parties to transactions and credit card usage”]; and
- Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as “your creditworthiness and credit history”].

Sample Clause A-2, Alternative 2:

We may disclose all of the information that we collect, as described [describe location in the notice, such as “above” or “below”].

A-3—Categories of information a financial institution discloses and parties to whom the financial institution discloses (institutions that do not disclose outside of the exceptions)

A financial institution may use this clause, as applicable, to meet the requirements of Sections 7A(2), (3), and (4) to describe the categories of nonpublic personal information about customers and former customers that the financial institution discloses and the categories of affiliates and nonaffiliated third parties to whom the financial institution discloses. A financial institution may use this clause if the financial institution does not disclose nonpublic personal financial information to any party, other than as permitted by the exceptions in Sections 15 and 16.

Sample Clause A-3:

We do not disclose any nonpublic personal financial information about our customers or former customers to anyone, except as permitted by law.

A-4—Categories of parties to whom a financial institution discloses (institutions that disclose outside of the exceptions)

A financial institution may use this clause, as applicable, to meet the requirement of Section 7A(3) to describe the categories of affiliates and nonaffiliated third parties to whom the financial institution discloses nonpublic personal information. This clause may be used if the financial institution discloses nonpublic personal financial information other than as permitted by the exceptions in Sections 14, 15 and 16, as well as when permitted by the exceptions in Sections 15 and 16.

Sample Clause A-4:

We may disclose nonpublic personal information about you to the following types of third parties:

- Financial service providers, such as [provide illustrative examples, such as “mortgage bankers, securities broker-dealers, and insurance agents”];
- Non-financial companies, such as [provide illustrative examples, such as “retailers, direct marketers, airlines, and publishers”]; and
- Others, such as [provide illustrative examples, such as “non-profit organizations”].

We may also disclose nonpublic personal information about you to third parties as permitted by law.

A-5-Service provider/joint marketing exception

A financial institution may use one of these clauses, as applicable, to meet the requirements of Section 7A(5) related to the exception for service providers and joint marketing in Section 14. If a financial institution discloses nonpublic personal information under this exception, the financial institution shall describe the categories of nonpublic personal information the financial institution discloses and the categories of third parties with which the financial institution has contracted.

Sample Clause A-5, Alternative 1:

We may disclose the following information to companies that perform marketing services on our behalf:

- Information we receive from you on applications or other forms, such as [provide illustrative examples, such as “your name, address, social security number, assets, and income”];
- Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as “your account balance, payment history, parties to transactions, and credit card usage”]; and
- Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as “your creditworthiness and credit history”].

Sample Clause A-5, Alternative 2:

We may disclose all of the information we collect, as described [describe location in the notice, such as “above” or “below”] to companies that perform marketing services on our behalf.

Sample Clause A-5, Alternative 3:

We may disclose the following information to other financial institutions with which we have joint marketing agreements:

- The following information we receive from you: “your name and contact information”;
- Information about your transactions with us or our affiliates, such as [provide illustrative examples of own transaction and experience information, such as “your account balance, payment history, parties to transactions, and credit card usage”].

A-6–Explanation of opt in (institutions that disclose to nonaffiliates outside of the exceptions)

A financial institution may use this clause, as applicable, to meet the requirement of Section 7A(6) to provide an explanation of the consumer’s right to authorize the disclosure of nonpublic personal financial information to nonaffiliated third parties, including the method(s) by which the consumer may exercise those rights. The financial institution may use this clause if the

financial institution discloses nonpublic personal financial information to nonaffiliated third parties other than as permitted by the exceptions in Sections 14, 15 and 16.

Sample Clause A-6:

We will not disclose nonpublic personal financial information about you to nonaffiliated third parties (other than as permitted by law) unless you authorize us to make that disclosure. Your authorization must be in writing or, if you agree, in electronic form. If you wish to authorize us to disclose your nonpublic personal financial information to nonaffiliated third parties, you may [describe the means to opt in, such as “complete and sign the enclosed, postage prepaid card and mail it to us.”]

A-7–Confidentiality and security (all institutions)

A financial institution may use this clause, as applicable, to meet the requirement of Section 7A(8) to describe its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A-7:

We restrict access to nonpublic personal information about you to [provide an appropriate description, such as “those employees who need to know that information to provide products or services to you”]. We maintain physical, electronic, and procedural safeguards that comply with state and federal regulations to guard your nonpublic personal information.