STATE OF VERMONT
DEPARTMENT OF FINANCIAL REGULATION
SECURITIES DIVISION

In the Matter of:

Repealing in part and retaining in part	)	
Order 06-23-S Applying Provisions of certain	)	
Regulations, Bulletins, Policy Statements and orders	)	**Docket 16-01-S**
In effect Prior to July 1, 2006 to the	)	
Vermont Uniform Securities Act	)	

WHEREAS, the Vermont Uniform Securities Act (2002), codified at 9 V.S.A. chapter 150 (the "Vermont Securities Act" or the "Act"), is effective as of July 1, 2006;

WHEREAS, the Commissioner of the Department of Financial Regulation (the "Commissioner") is charged with the administration of the Act:

WHEREAS, the Act authorizes the Commissioner to issue orders, rules, and interpretive opinions as the Commissioner deems necessary and appropriate to carry out the provisions and purposes of the Act;

WHEREAS, the Commissioner promulgated Order 06-43-S Applying Certain Provisions of Certain Regulations, Bulletins, Policy Statements and Orders (the "Transition Order") on July 1, 2006 in order to provide certain regulations that apply on and after the effective date of the Vermont Securities Act and until such time as such provisions are replaced, amended, or repealed;

WHEREAS, the Commissioner subsequently promulgated Rule S-2016-1, the Vermont Securities Regulations ("V.S.R.") providing regulations under the authority of the Act intended to replace the Transition Order through the Administrative Procedure Act rule-making process; and

WHEREAS, the Commissioner finds it necessary and appropriate in the public interest to retain exhibit 5.11 of the Transition Order until such time as that provision can be promulgated as a rule;

NOW, THEREFORE, IT IS HEREBY ORDERED THAT:

The Transition Order, Order 06-43-S is hereby terminated in its entirety, with the exception of the provisions contained below. The following provision from Exhibit 5.11 of Order 06-43-S will remain in effect:

PRIVACY OF CONSUMER FINANCIAL AND HEALTH INFORMATION

Table of Contents

26. [reserved]
27. Procedures to safeguard customer records and information

Appendix to S-01-1 - Sample Clauses

Section 1. [reserved]

Section 2. Purpose, scope and compliance

(a) *Purpose* This Exhibit 5.1 to Order 06-43-S (the "Exhibit") governs the treatment of nonpublic personal information about individuals by the financial institutions listed in paragraph (b) of this section. This Exhibit:

(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 individuals to nonaffiliated third parties; and

(3) Provides a method for consumers to prevent a financial institution from disclosing that information, subject to the exceptions in sections 14, 15, 16 and 17 of this Exhibit and subject to the federal Fair Credit Reporting Act and Vermont Fair Credit Reporting Act.

(b) *Scope.* This Exhibit applies to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes from the financial institutions listed below. This Exhibit does not apply to information about companies or about individuals who obtain financial products or services for business, commercial, or agricultural purposes. This Exhibit applies to broker-dealers and investment advisers that are registered or required to be registered with the Department. These entities are referred to in this Exhibit as "you."

(c) *Health Information.* This Exhibit applies to all nonpublic personal health information.

(d) *Compliance*
(1) A financial institution subject to this Exhibit regardless of its jurisdiction of domicile shall comply with this Exhibit for all transactions with Vermont consumers.

Section 3. Rule of construction.

The examples in this Exhibit and the sample clauses in the Appendix of this Exhibit provide guidance concerning the Exhibit'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 Exhibit.

Section 4. Definitions.

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

(a) *Affiliate* means any company that controls, is controlled by, or is under common control with another financial institution or another company. In addition, a broker-dealer or investment adviser will be deemed an affiliate of a company for the purposes of this Exhibit if:

(1) that company is regulated under Title V of the Gramm-Leach-Bliley Act (Pub. L. No. 106-102, 133 Stat. 1338(1999)) by the Federal Trade Commission or by a federal functional regulator; and

(2) rules adopted by the Federal Trade Commission or another federal functional regulator under Title V of the Gramm-Leach-Bliley Act (Pub. L. No. 106-102, 133 Stat. 1338(1999)) treat the broker-dealer or investment adviser as an affiliate of that company.

(b) *Broker-dealer* has the same meaning as in Title 9 V.S.A. § 5102(3).

(c) (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.*

(i) *Reasonably understandable.* You make your notice reasonably understandable if you:

(A) Present the information in the notice in clear, concise sentences, paragraphs, and sections;

(B) Use short explanatory sentences or bullet lists whenever possible;

(C) Use definite, concrete, everyday words and active voice whenever possible;

(D) Avoid multiple negatives;

(E) Avoid legal and highly technical business terminology whenever possible;

(F) Avoid explanations that are imprecise and readily subject to different interpretations; and

(G) Avoid contradictory, confusing or misleading language.

(ii) *Designed to call attention.* You design your notice to call attention to the nature and significance of the information in it if you:

(A) Use a plain-language heading to call attention to the notice;

(B) Use a typeface and type size that are easy to read;

(C) Provide wide margins and ample line spacing;

(D) Use boldface or italics for key words; and

(E) Use distinctive type size, style, and graphic devices, such as shading or sidebars when you combine your notice with other information.

(iii) *Notices on web sites.* If you provide a notice on a web page, you design your notice to call attention to the nature and significance of the information in it if you use 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 you either:

(A) Place the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(B) Place 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.

(d) *Collect* means to obtain information that you organize 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.

(e) *Commissioner* means the commissioner of the Vermont Department of Banking, Insurance, Securities and Health Care Administration.

(f) *Company-means* any corporation, limited liability company, business trust, general or limited partnership, association, sole proprietorship or similar organization.

(g) (1) *Consumer* means an individual who seeks to obtain, obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, and about whom you have nonpublic personal information, or that individual's legal representative.

(2) *Examples.* (i) An individual is your consumer if he or she provides nonpublic personal information to you in connection with obtaining or seeking to obtain brokerage services or investment advisory services, whether or not you provide brokerage services to the individual or establish a continuing relationship with the individual.

(ii) An individual is not your consumer if he or she provides you only with his or her name, address, and general areas of investment interest in connection with a request for a prospectus, an investment adviser brochure, or other information about financial products or services.

(iii) An individual is not your consumer if he or she has an account with another broker-dealer (the introducing broker-dealer) that carries securities for the individual in a special omnibus account with you (the clearing broker-dealer) in the name of the introducing broker-dealer, and when you receive only the account numbers and transaction information of the introducing broker-dealer's consumers in order to clear transactions.

(iv) An individual who is a consumer of another financial institution is not your consumer solely because you act as agent for, or provide processing or other services to, that financial institution.

(v) An individual is not your consumer solely because he or she has designated you as trustee for a trust.

(vi) An individual is not your consumer solely because he or she is a beneficiary of a trust for which you are a trustee.

(vii) An individual is not your consumer solely because he or she is a participant or a beneficiary of an employee benefit plan that you sponsor or for which you act as a trustee or fiduciary.

(h) *Consumer reporting agency* has the same meaning as in section 603(f) of the federal Fair Credit Reporting Act (15 U.S.C. § 168la(f)) and shall include any "credit reporting agency" within the meaning of9 V.S.A. § 2480a(3).

(i) *Control* of a company means the power to exercise a controlling influence over the management or policies of a company whether through ownership of securities, by contract, or otherwise. Any person who owns beneficially, either directly or through one or more controlled companies, more than 25 percent of the voting securities of any company is presumed to control the company. Any person who does not own more than 25 percent of the voting securities of any company will be presumed not to control the company. Any presumption regarding control may be rebutted by evidence.

(j) *Customer* means a consumer who has a customer relationship with you.

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

(2) *Examples.* (i) *Continuing relationship.* A consumer has a continuing relationship with you if:

(A) The consumer has a brokerage account with you, or if a consumer's account is transferred to you from another broker-dealer;

(B) The consumer has an investment advisory contract with you (whether written or oral);

(C) The consumer holds an investment product through you, such as when you act as a custodian for securities or for assets in an Individual Retirement Arrangement;

(D) The consumer purchases a variable insurance product from you;

(E) The consumer has an account with an introducing broker-dealer that clears transactions with and for its customers through you on a fully disclosed basis;

(F) You hold securities or other assets as collateral for a loan made to the consumer, even if you did not make the loan or do not effect any transactions on behalf of the consumer; or

(G) You regularly effect or engage in securities transactions with or for a consumer even if you do not hold any assets of the consumer.

(ii) *No continuing relationship.* A consumer does not, however, have a continuing relationship with you if you open an account for the consumer solely for the purpose of liquidating or purchasing securities as an accommodation, *i.e.*, on a one-time basis, without the expectation of engaging in other transactions.

(l) *Department* means the Vermont Department of Banking, Insurance, Securities and Health Care Administration.

(m) (1) *Financial institution* means any institution 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)).

(2) *Financial institution* does not include:

(i) 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.);*

(ii) 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

(iii) 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.

(n) (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 your evaluation or brokerage of information that you collect in connection with a request or an application from a consumer for a financial product or service.

(o) *Health Care* means:

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

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

(ii) 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.

(p) *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.

(q) *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.

(r) *Investment adviser* has the same meaning as in Title 9 V.S.A. § *5102(15); federal covered investment adviser* has the same meaning as in 9 V.S.A. § 5102(6). For purposes of this Exhibit, the term *investment adviser* shall include a federal covered investment adviser.

(s) (1) *Nonaffiliated third party* means any person except:

(i) Your affiliate; or

(ii) A person employed jointly by you and any company that is not your 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 your or your 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) or insurance company investment activities of the type described in section 4(k)(4)(1) of the Bank Holding Company Act (12 U.S.C. § 1843(k)(4)(H) and(I)) and also includes Vermont merchant banks as described in 8 V.S.A. § 12603.

(t) *Nonpublic personal information* means nonpublic personal financial information and nonpublic personal health information.

(u) (1) *Nonpublic personal financial information* means:

(i) Personally identifiable financial information; and

(ii) 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 information.

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

(i) Health information;

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

(iii) 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 information.

(3) *Examples of lists.* (i) 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 information, such as account numbers.

(ii) 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 information, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

(v) *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.

(w) (1) *Personally identifiable financial information* means any information:

(i) A consumer provides to you to obtain a financial product or service from you;
(ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or

(iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

(2) *Examples.*

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

(A) Information a consumer provides to you on an application to obtain a loan, credit card, or other financial product or service;

(B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;

(C) The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;

(D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;

(E) Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on a loan or servicing a loan;

(F) Any information you collect through an Internet "cookie" (an information collecting device from a web server); and

(G) Information from a consumer report.

(ii) *Information not included.* Personally identifiable financial information doesnot include:

(A) Health information;

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

(x)(l) *Publicly available information* means any information that you reasonably believe is lawfully made available to the general public from:

(i) Federal, State, or local government records;

(ii) Widely distributed media; or

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

(2) *Examples.* (i) *Reasonable belief*

(A) You have a reasonable belief that information about your consumer is lawfully made available to the general public if you have confirmed, or your consumer has represented to you, that the information is publicly available from a source described in paragraphs (x)(l)(i) - (iii) of this section;

(B) You have a· reasonable belief that information about your consumer is made available to the general public if you have taken steps to submit the information, in accordance with your internal procedures and policies and with applicable law, to a keeper of federal,

State, or local government records that is required by law to make the information publicly available.

(C) You have a reasonable belief that an individual's telephone number is lawfully made available to the general public if you have located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

(D) You do not have a reasonable belief that information about a consumer is publicly available solely because that information would normally be recorded with a keeper of federal, State, or local government records that is required by law to make the information publicly available, if the consumer has the ability in accordance with applicable law to keep that information nonpublic, such as where a consumer may record a deed in the name of a blind trust.

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

(iii) *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.

(y) *You* means:

(1) Any broker-dealer registered or required to be registered with the Department; and

(2) Any investment adviser registered or required to be registered with the Department including a federal covered investment advisor who makes the notice filing, or is required to make the notice filing, provided for in 9 V.S.A. § 5405.

Subpart A-Privacy and Opt-in Notices for Nonpublic Personal Information

Section 5. Initial privacy notice to consumers required.

(a) *Initial notice requirement.* You must provide a clear and conspicuous notice that accurately reflects your privacy policies and practices with respect to nonpublic personal information to:

(1) *Customer.* An individual who becomes your customer, not later than when you establish a customer relationship, except as provided in paragraph (e) of this section; and

(2) *Consumer.* A consumer, before you disclose any nonpublic personal information about the consumer to any nonaffiliated third party, if you make such a disclosure other than as authorized by Sections 15, 16 and 17 of this Exhibit.

(b) *When initial notice to a consumer is not required.* You are not required to provide an initial notice to a consumer under paragraph (a)(2) of this section if:

(1) You do 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 you do 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 you and your other affiliates.

(c) *When you establish a customer relationship.*

(l) *General rule.* You establish a customer relationship when you and the consumer enter into a continuing relationship.

(2) *Special Rule for Loans.* You do not have a customer relationship with a consumer if you buy a loan made to the consumer but do not have the servicing rights for that loan.

(3) *Examples of establishing customer relationship.* You establish a customer relationship when the consumer:

(i) Effects a securities transaction with you or opens a brokerage account with you under your procedures;

(ii) Opens a brokerage account with an introducing broker-dealer that clears transactions with and for its customers through you on a fully disclosed basis; or

(iii) Enters into an advisory contract with you (whether in writing or orally).

(d) *Existing customers.* When an existing customer obtains a new financial product or service from you that is to be used primarily for personal, family, or household purposes, you satisfy the initial notice requirements of paragraph (a) of this section as follows:

(1) You may provide a revised privacy notice, under Section 9, that covers the customer's new financial product or service; or

(2) If the initial, revised, or annual notice that you most recently provided to that customer was accurate with respect to the new financial product or service, you do not need to provide a new privacy notice under paragraph (a) of this section.

(e) *Exceptions to allow subsequent delivery of notice.*

(1) You may provide the initial notice required by paragraph (a)(l) of this section within a reasonable time after you establish a customer relationship if:

(i) Establishing the customer relationship is not at the customer's election;

(ii) Providing notice not later than when you establish a customer relationship would substantially delay the customer's transaction and the customer agrees to receive the notice at a later time; or

(iii) A nonaffiliated broker-dealer or investment adviser establishes a customer relationship between you and a consumer without your prior knowledge.

(2) *Examples of exceptions.*

(i) *Not at customer's election.* Establishing a customer relationship is not at the customer's election if the customer's account is transferred to you by a trustee selected by the Securities Investor Protection Corporation ("SIPC") and appointed by a United States Court.

(ii) *Substantial delay of customer's transaction.* Providing notice not later than when you establish a customer relationship would substantially delay the customer's transaction when you and the individual agree over the telephone to enter into a customer relationship involving prompt delivery of the financial product or service.

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

(f) *Delivery.* When you are required to deliver an initial privacy notice by this section, you must deliver it according to Section 10. If you use a short-form initial notice for non-customers according to Section 7(d), you may deliver your privacy notice according to Section 7(d)(3).

Section 6. Annual privacy notice to customers required.

(a) (l) *General rule.* You must provide a clear and conspicuous notice to customers that accurately reflects your 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 12 consecutive months during which that relationship exists. You may define the 12-consecutive-month period, but you must apply it to the customer on a consistent basis.

(2) *Example.* You provide a notice annually if you define the 12-consecutive-month period as a calendar year and provide the annual notice to the customer once in each calendar year following the calendar year in which you provided the initial notice. For example, if a customer opens an account on any day of year 1, you must provide an annual notice to that customer by December 31 of year 2.

(b)(l) *Termination of customer relationship.* You are not required to provide an annual notice to a former customer A former customer is an individual with whom you no longer have a continuing relationship.

(2) *Examples.* You no longer have a continuing relationship with a customer if:

(i) The individual's brokerage account is closed;

(ii) The individual's investment advisory contract is terminated; or

(iii) You no longer have a continuing relationship with an individual if the individual's last known address according to your records is deemed invalid. An address of record is deemed invalid if mail sent to that address by you has been

returned by the postal authorities as undeliverable and if subsequent attempts by you to obtain a current valid address for the individual have been unsuccessful.

(c) *Special Rule for Loans.* If you-do not have a customer relationship with a consumer under the special provision for loans in Section 5(c)(2), then you need not provide an annual notice to that consumer under this section.

(d) *Delivery.* When you are required to deliver an annual privacy notice by this section, you must deliver it according to Section 10.

Section 7. Information to be included in privacy notices.

(a) *General rule.* The initial, annual, and revised privacy notices that you provide under Sections 5, 6 and 9 must include each of the following items of information that applies to you or to the consumers to whom you send your privacy notice, in addition to any other information you wish to provide:

(1) The categories of nonpublic personal information that you collect;

(2) The categories of nonpublic personal information that you disclose;

(3) The categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information, other than those parties to whom you disclose information under Sections 15, 16 and 17;

(4) The categories of nonpublic personal information about your former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your former customers, other than those parties to whom you disclose information under Sections 15, 16 and 17;

(5) If you disclose nonpublic personal financial information to a third party under Section 14 (and no other exception in Sections 15 or 16 applies to that disclosure), a separate statement of the categories of information, as limited by Section 14, you disclose and the categories of nonaffiliated third parties with whom you have contracted;

(6) An explanation of the consumer's right to opt in under Section 11(a) prior to the disclosure of nonpublic personal financial information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right at any time;

(7) Any disclosures that you make under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. § 168la(d)(2)(A)(iii)) and the federal implementing regulations as modified by 15 U.S.C. § !681t(b)(2) and the Vermont Fair Credit Reporting Act, 9 V.S.A. § 2480e;

(8) Your policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; and

(9) Any disclosure that you make under paragraph (b) of this section.

(b) *Description of parties subject to exceptions.* If you disclose nonpublic personal information to third parties as authorized under Sections 15, 16 and 17, you are not required to list those exceptions in the initial or annual privacy notices required by Sections 5 and 6. When describing the categories with respect to those parties, you are required to state only that you make disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.

(c) *Examples.* (1) *Categories of nonpublic personal financial information that you collect.* You satisfy the requirement to categorize the nonpublic personal financial information that you collect if you categorize the information according to the source of the information, as applicable:

(i) Information from the consumer;

(ii) Information about the consumer's transactions with you or your affiliates;

(iii) Information about the consumer's transactions with nonaffiliated third parties; and

(iv) Information from a consumer-reporting agency.

(2) *Categories of nonpublic personal financial information you disclose.*

(i) You satisfy the requirement to categorize the nonpublic personal financial information that you disclose if you list the categories described in paragraph (c)(l) of this section, as applicable, and a few examples to illustrate the types of information in each category. These might include:

(A) Information from the consumer, including application information, such as assets and income and identifying information, such as name, address and social security number;

(B) Transaction information, such as information about balances, payment history and parties to the transaction; and

(C) Information from consumer reports, such as a consumer's creditworthiness and credit history.

(ii) If you reserve the right to disclose all of the nonpublic personal financial information about consumers that you collect, you may simply state that fact without describing the categories or examples of the nonpublic personal financial information you disclose.

(iii) You do not adequately categorize the information you disclose if you use only general terms, such as transaction information about the consumer.

(3) *Categories of affiliates and nonaffiliated third parties to whom you disclose.*

(i) You satisfy the requirement to categorize the affiliates and nonaffiliated third parties to whom you disclose nonpublic personal financial information if you identify the types of businesses in which they engage.

(ii) Types of businesses may be described by general terms only if you use a few illustrative examples of significant lines of business. For example, you may use the term financial products or services if it includes appropriate examples of significant lines of businesses, such as life insurer, consumer banking or securities brokerage.

(iii) You may categorize the affiliates and nonaffiliated third parties to which you disclose nonpublic personal financial information about consumers using more detailed categories.

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

(i) Subject to the limitation in Section 14, list the categories of nonpublic personal financial information you disclose, using the same categories and examples you used to meet the requirements of paragraph (a)(2) of this section, as applicable; and

(ii) State whether the third party is:

(A) A service provider that performs marketing services on your behalf or on behalf of you and another financial institution; or

(B) A financial institution with which you have a joint marketing agreement.

(5) *Simplified notices.* If you do not disclose, and do 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, you may simply state that fact, in addition to the information you must provide under paragraphs (a)(l), (a)(8), (a)(9), and (b) of this section.

(6) *Confidentiality and security.* You describe your policies and practices with respect to protecting the confidentiality and security of nonpublic personal financial information if you do both of the following:

(i) Describe in general terms who is authorized to have access to the information; and

(ii) State whether you have security practices and procedures in place to ensure the confidentiality of the information in accordance with your policy. You are not required to describe technical information about the safeguards you use.

(d) *Short-form initial notice with opt-in notice for non-customers.*

(1) You may satisfy the initial notice requirements in Section 5(a)(2) and Section 8(d) for a consumer who is not a customer by providing a short-form initial notice at the same time as you deliver an opt-in notice as required in Section 8.

(2) A short-form initial notice must:

(i) Be clear and conspicuous;

(ii) State that your privacy notice is available upon request; and

(iii) Explain a reasonable means by which the consumer may obtain the privacy notice.

(3) You must deliver your short-form initial notice according to Section 10. You are not required to deliver your privacy notice with your short-form initial notice. You instead may simply provide the consumer a reasonable means to obtain your privacy notice. If a consumer who receives your short-form notice requests your privacy notice, you must deliver your privacy notice according to Section 10.

(4) *Examples of obtaining privacy notice.* You provide a reasonable means by which a consumer may obtain a copy of your privacy notice if you:

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

(ii) For a consumer who conducts business in person at your office, maintain copies of the notice on hand that you provide to the consumer immediately upon request.

(e) *Future disclosures.* Your notice may include:

(1) Categories of nonpublic personal financial information that you reserve the right to disclose in the future, but do not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom you reserve the right in the future to disclose, but to whom you do 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 the Appendix of this Exhibit.

Section 8. Form of opt-in notice to consumers; opt-in methods.

(a) (1) *Form of opt-in notice.* If you are required to provide an opt-in notice under Section 11(a) then you may not disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party unless you:

(i) Provide 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 you disclose nonpublic personal financial information;

(ii) Identify the financial product or services that the consumer obtains from the financial institution, either singly or jointly, to which the opt-in direction would apply;

(iii) Identify the methods by which the consumer may subsequently revoke the opt-in direction;

(iv) Clearly and conspicuously request in writing or in electronic form that the consumer affirmatively authorize such disclosure; and

(v) Obtain from the consumer such affirmative consent and such consent has not been withdrawn.

(2) *Unreasonable revocation of opt-in direction means.* You *do not* provide a reasonable means of revoking an opt-in direction if:

(i) The only means of revoking an opt-in direction is for the consumer to write his or her own letter to effect a revocation; or

(ii) The only means revoking an opt-in direction as described in any notice subsequent to the initial notice is to use a check-off box that you provided with the initial notice but did not include with the subsequent notice.

(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 your rights if you 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 you, the opt-in direction that applied to the former relationship does not apply to the new relationship.

(4) *Joint relationships.* If two or more consumers jointly obtain a financial product or service from you, you 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 product or service.

(5) *Aggregate Lists.* You may not disclose any aggregate list of consumers containing or derived from nonpublic personal financial information to a nonaffiliated third party unless you have satisfied, for each consumer on the list, the requirements of subdivisions (i), (ii), (iii), (iv) and (v) of (a)(1) of this section.

(6) *Exceptions.* This section shall not restrict you from disclosing nonpublic personal financial information as authorized in Sections 14, 15, 16 and 17.

(7) *Record Retention.* You must retain the opt-in authorization or a copy thereof in the record of the consumer who is the subject of disclosure of nonpublic personal financial information.

(b) *Delivery.* When you are required to deliver an opt-in notice by this section, you must deliver it according to Section 10.

(c) *Same form as initial notice permitted.* You may provide the opt-in notice together with or on the same written or electronic form as the initial notice you provide in accordance with Section 5.

(d) *Initial notice required when opt-in notice delivered subsequent to initial notice.* If you provide the opt-in notice after the initial notice in accordance with Section 5, you must also include a copy of the initial notice with the opt-in notice in writing or, if the consumer agrees, electronically.

Section 9. Revised privacy notices.

(a) *General rule.* Except as otherwise authorized in this Exhibit, you must not, directly or through any affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that you provided to that consumer under Section 5, unless:

(1) You have provided to the consumer a clear and conspicuous revised notice that accurately describes your policies and practices;

(2) You have provided to the consumer a new opt-in notice; and

(3) The consumer provides an affirmative consent to the disclosures described in the notice.

(b) *Examples.*

(1) Except as otherwise permitted by Sections 14, 15 and 16, you must provide a revised notice before you:

(i) Disclose a new category of nonpublic personal financial information to any nonaffiliated third party;

(ii) Disclose nonpublic personal financial information to a new category of nonaffiliated third party; or

(iii) Disclose 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 you disclose nonpublic personal financial information to a new nonaffiliated third party that you adequately described in your prior notice.

(c) *Delivery.* When you are required to deliver a revised privacy notice by this section, you must deliver it according to Section I 0.

(d) *Fair Credit Reporting Acts.* Nothing in this Exhibit shall relieve you 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. Delivering privacy and opt-in notices.

(a) *How to provide notices.* You must provide any notice that this Exhibit 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.* You may reasonably expect that a consumer will receive actual notice if you:

(i) Hand-deliver a printed copy of the notice to the consumer;

(ii) Mail a printed copy of the notice to the last known address of the consumer;

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

(iv) For an isolated transaction with the consumer, such as an ATM transaction, post the notice on the ATM screen and require 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.* You may *not,* however, reasonably expect that a consumer will receive actual notice of your privacy policies and practices if you:

(i) Only post a sign in your branch or office or generally publish advertisements of your privacy policies and practices; or

(ii) Send the notice via electronic mail to a consumer who does not obtain a financial product or service from you electronically.

(c) *Annual notices only.* You may reasonably expect that a customer will receive actual notice of your annual privacy notice if:

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

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

(d) *Oral description of notice insufficient.* You may not provide any notice required by this Exhibit 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, you must provide the initial notice required by Section 5(a)(l), the annual notice required by Section 6(a), 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.* You provide a privacy notice to the customer so that the customer can retain it or obtain it later if you:

(i) Hand-deliver a printed copy of the notice to the customer;

(ii) Mail a printed copy of the notice to the last known address of the customer; or

(iii) Make your 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.* You may provide a joint notice from you and one or more of your affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to you and the other institutions. You may also 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 you, you may satisfy the initial, annual, and revised notice requirements of Sections 5(a), 6(a) and (9)(a) respectively by providing one notice to those consumers jointly.

Subpart B-Limits on Disclosures of Financial Information

Section 11. Limits on disclosure of nonpublic personal financial information to nonaffiliated third parties.

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

(1) You have provided to the consumer an initial notice as required under Section 5;

(2) You have provided to the consumer an opt-in notice under Section 8 of this Exhibit; and

(3) The consumer has authorized the disclosure in writing or, if the consumer agrees, electronically.

(b) *Opt in definition.* "Opt in" means the written, or if the consumer agrees, electronic authorization by the consumer allowing you to disclose nonpublic personal financial information about that consumer to a nonaffiliated third party, other than as permitted by Sections 14, 15, and 16.

(c) *Application of Opt in to all consumers and all nonpublic personal financial information.*

(1) You must comply with this section, regardless of whether you and the consumer have established a customer relationship.

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

(d) *Partial Opt in.* You 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 you receive under an exception.* If you receive nonpublic personal financial information from a nonaffiliated financial institution under an exception in Sections 15 or 16, your disclosure and use of that information is limited as follows:

(i) You may disclose the information to the affiliates of the financial institution from which you received the information;

(ii) · You may disclose the information to your affiliates, but your affiliates may, in tum, disclose and use the information only to the extent that you may disclose and use the information; and

(iii) You 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 you received the information.

(2) *Example.* If you receive a customer list from a nonaffiliated financial institution in order to provide account-processing services under the exception in Section 15(a), you may disclose that information under any exception in Sections 15 or 16 in the ordinary course of business in order to provide those services. You could also disclose that information in response to a properly authorized subpoena or in the ordinary course of business to your attorneys,

accountants, and auditors. You could not disclose that information to a third party for marketing purposes or use that information for your own marketing purposes.

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

(i) To the affiliates of the financial institution from which you received the information;

(ii) To your affiliates, but your affiliates may, in turn, disclose the information only to the extent that you can disclose the information; and

(iii) To any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which you received the information.

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

(i) You may use that list for your own purposes; and

(ii) You may disclose that list to another nonaffiliated third party only if the financial institution from which you purchased the list could have lawfully disclosed the list to that third party. That is, you may disclose the list in accordance with the privacy policy of the financial institution from which you received the list, as limited by the absence or limitation of the opt-in direction of each consumer whose nonpublic personal financial information you intend to disclose, and you may disclose the list in accordance with an exception in Sections 15 or 16, such as in the ordinary course of business to your attorneys, accountants, or auditors.

(c) *Information you disclose under an exception.* If you disclose nonpublic personal financial information to a nonaffiliated third party under an exception in Sections 15 or 16, the third party may disclose and use that information only as follows:

(1) The third party may disclose the information to your 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 you disclose outside of an exception.* If you disclose nonpublic personal financial information to a nonaffiliated third party other than under an exception in Sections 15 or 16, the third party may disclose the information only:

(1) To your affiliates;

(2) To its affiliates, but its 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 you made it directly to that person.

(e) *Fair Credit Reporting Acts.* Nothing in this Exhibit shall authorize you to make any disclosures to an affiliate not otherwise in compliance with the requirement of the federal Fair Credit Reporting Act or regulations promulgated thereunder or the Vermont Fair Credit

Reporting Act or regulations promulgated thereunder, 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.* You must 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 credit card account, deposit account, or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer. You shall not provide an account number or similar form of access number or access code, in an encrypted form.

(b) *Exceptions.* Paragraph (a) of this section does not apply if you disclose an account number or similar form of access number or access code:

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

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

(c) *Example-Account number.*

(1) An account number, or similar form of access number or access code, includes a number or code in an encrypted form.

Subpart C-Exceptions

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 you provide nonpublic personal information to a nonaffiliated third party to perform services for you or functions on your behalf, if you:

(i) Provide the initial notice in accordance with Section 5;

(ii) Enter 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 you 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

(iii) For joint marketing agreements,

(A) you provide 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. § 168la(d)(2)(A)(i) and the Vermont Fair Credit Reporting Act, 9 V.S.A. § 2480a(2)(A); and,

(B) in the event health information is provided as own transaction or experience information as defined in (A) of this subdivision (iii), complies with section 20 of this rule.

(2) *Examples.*

(i) If you disclose nonpublic personal information under this section to a financial institution with which you perform joint marketing, your contractual agreement with that institution meets the requirements of paragraph (a)(1)(ii) 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.

(ii) If you comply with the provisions of Section 14(a)(l)(i), (ii) of this Exhibit, you may provide nonpublic personal information to a service provider that is a nonaffiliated third party agent of yours to enable the agent to offer, renew or service products on your behalf Such disclosure shall not be subject to the limitations of paragraph (a)(1)(iii) of this section.

(b) *Service may include joint marketing.* The services a nonaffiliated third party performs for you under paragraph (a) of this section may include marketing of your own products or services or marketing of financial products or services offered pursuant to joint agreements between you and one or more financial institutions.

(c) *Joint agreement. Definition.* For purposes of this section, *joint agreement* means a written contract pursuant to which you 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 and servicing transactions at consumer's request.* The requirements for initial notice in Section 5(a)(2), for the opt-in requirements in Sections 8 and 11, and for service providers and joint marketing in Section 14, do not apply if you disclose nonpublic personal financial information as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or in connection with:

(1) Processing or servicing a financial product or service that a consumer requests or authorizes;

(2) Maintaining or servicing the consumer's account with you, 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

(1) Required, or is one of the lawful or appropriate methods, to enforce your 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:

(i) 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 service or financial product;

(ii) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

(iii) To provide a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product to the consumer or the consumer's agent or broker;

(iv) To accrue or recognize incentives or bonuses associated with the transaction that are provided by you or any other party;

(v) 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

(vi) In connection with:

(A) 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;

(B) The transfer of receivables, accounts, or interests therein; or

(C) 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 in Section 5(a)(2) and for the opt-in requirements in Sections 8, 11 and service providers and joint marketing under Section 14 do not apply when you disclose 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) (i) To protect the confidentiality or security of your records pertaining to the consumer, service, product, or transaction;

(ii) To protect against or prevent actual or potential fraud or unauthorized transactions;

(iii) For required institutional risk control or for resolving consumer disputes or inquiries;

(iv) To persons holding a legal or beneficial interest relating to the consumer; or

(v) 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 you, persons that are assessing your compliance with industry standards, and your 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), self-regulatory organizations or for an investigation on a matter related to public safety;

(5) (i) To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.),* or

(ii) 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 such business or unit;

(7) (i) To comply with federal, state, or local laws, rules and other applicable legal requirements;

(ii) To comply with a properly authorized civil, criminal, or regulatory investigation, or subpoena or summons by federal, state, or local authorities;

(iii) To respond to judicial process or government regulatory authorities having jurisdiction over you for examination, compliance, or other purposes as authorized by law; or

(8) In the administration of an order or proceeding under Chapter 150 of Title 9.

(b) *Examples of revocation of consent.* A consumer may revoke consent by subsequently exercising the right to prevent future disclosures of nonpublic personal financial information as permitted under Section 8(a).

Subpart D-Rules for Health Information

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

(a) *General rule.* You 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 the subject of a requested disclosure.

(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 rule 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 Exhibit; and

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

(c) *Additional Functions.* 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) *Authorization requirement.* A valid authorization to disclose nonpublic personal health information pursuant to this Subpart D 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 you disclose 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) *Time Limits.* An authorization for the purposes of this Subpart D 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) *Revocation of authorization.* A consumer or customer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Subpart D at any time, subject to your rights if you acted in reliance on the authorization prior to notice of the revocation.

(d) *Record retention.* · You 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 I 0, 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 you intend to disclose protected health information pursuant to Section 17(a).

Section 20. Relationship to Federal Rules.

Irrespective of whether you are subject to the federal Health Insurance Portability and Accountability Act privacy rule as promulgated by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164, (the "federal rule"), if you comply with all requirements of the federal rule and its effective date provision, you shall be deemed to be in compliance with the provisions of this Subpart D; provided, however, you shall be prohibited from making disclosures under the provisions of 45 C.F.R. § 164.514(e)(2) without the consumer's prior written consent. Nothing in this Exhibit 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 article shall preempt or supersede existing state law related to medical records, health or insurance information privacy.

Subpart E- Additional Provisions

Section 22. Protection of Fair Credit Reporting Acts.

(a) *Transaction and experience information.* No inference shall be drawn on the basis of the provisions of this Exhibit regarding whether information is transaction or experience information under Section 603 of federal Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.).

(b) *Vermont Fair Credit Reporting Act.* Nothing in this Exhibit 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 Exhibit regarding whether information is transaction or experience information under section 2480a(2) of the Vermont Fair Credit Reporting Act. This Exhibit 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) *No opt-in discrimination.* You shall not unfairly discriminate against a consumer or customer because that consumer or customer has not granted authorization for the disclosure of his or her nonpublic personal financial information pursuant to the provisions of this Exhibit.

(b) *No health opt-in discrimination.* You shall not unfairly discriminate against a consumer or customer because that consumer or customer has not granted authorization for the disclosure of his or her nonpublic personal health information pursuant to the provisions of this Exhibit.

Section 24. Violations.

In addition to any other sanctions available to the commissioner under Vermont law for violations of this Exhibit, any violation of this Exhibit shall be deemed an unfair method of competition or an unfair or deceptive act or practice in the conduct of a broker-dealer or investment adviser for the purposes of Chapter 150 of Title 9 V.S.A.

Section 25. Severability.

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

Section 26. [reserved]

Section 27. Procedures to safeguard customer records and information.

Every broker-dealer and every investment adviser registered with the Department must adopt policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. These policies and procedures must be reasonably designed to:

(a) Insure the security and confidentiality of customer records and information;

(b) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and

(c) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Appendix - 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 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 you collect (all institutions)

You may use this clause, as applicable, to meet the requirement of Section 7(a)(l) to describe the categories of nonpublic personal financial information you collect.

Sample Clause A-1:

We collect nonpublic personal financial 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 you disclose (institutions that disclose outside of the exceptions)

You may use one of these clauses, as applicable, to meet the requirement of Section 7(a)(2) to describe the categories of nonpublic personal financial information you disclose. You may use these clauses if you disclose 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 you disclose and parties to whom you disclose (institutions that do not disclose outside of the exceptions)

You may use this clause, as applicable, to meet the requirements of Section 7(a)(2), (3), and (4) to describe the categories of nonpublic personal financial information about customers and former customers that you disclose and the categories of affiliates and nonaffiliated third parties

to whom you disclose. You may use this clause if you do 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 you disclose (institutions that disclose outside of the exceptions)

You may use this clause, as applicable, to meet the requirement of Section 7(a)(3) to describe the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal financial information. You may use this clause if you disclose 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 financial 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 financial information about you to nonaffiliated third parties as permitted by law.

A-5. Service provider/joint marketing exception

You may use one of these clauses, as applicable, to meet the requirements of Section 7(a)(5) related to the exception for service providers and joint marketers in Section 14. If you disclose nonpublic personal information under this exception, you must describe the categories of nonpublic personal financial information you disclose and the categories of third parties with whom you have contracted.

Sample Clause A-5, Alternative 1:

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements.

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"1;*

- 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"1;* 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"1* to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

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 right (institutions that disclose to non affiliates outside of the exceptions)

You may use this clause, as applicable, to meet the requirement of Section 7(a)(6) to provide an explanation of the consumer's right to opt in to the disclosure of nonpublic personal financial information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. You may use this clause if you disclose 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-b:
We will not disclose nonpublic personal financial information about you to nonaffiliated third parties (other than disclosures permitted by law), unless you authorize us to make those disclosures. 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 a reasonable means of opting in, such as "sign the attached, postage prepaid card and mail it to us*"].

A-7. Confidentiality and security (all institutions)

You may use this clause, as applicable, to meet the requirement of Section 7(a)(8) to describe your 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 federal standards to guard your nonpublic personal information.

This Order will be effective as of July 1, 2016 and remain in effect unless and until subsequently amended or rescinded by order or regulation adopted under the Vermont Securities Act.

Effected at Montpelier, Vermont this 1st day of June, 2016

Susan L. Donegan, Commissioner
Department of Financial Regulation