SENATE DOCKET, NO. 353 FILED ON: 1/16/2017

SENATE . . . . . No. 116

The Commonwealth of Massachusetts

PRESENTED BY:

James B. Eldridge

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act protecting the privacy of consumer financial information.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	
James B. Eldridge	*Middlesex and Worcester*	
Robert M. Koczera	*11th Bristol*	*2/2/2017*
James Arciero	*2nd Middlesex*	*2/3/2017*

SENATE DOCKET, NO. 353 FILED ON: 1/16/2017

SENATE . . . . . No. 116

By Mr. Eldridge, a petition (accompanied by bill, Senate, No. 116) of James B. Eldridge, Robert M. Koczera and James Arciero for legislation to protect the privacy of consumer financial information. Consumer Protection and Professional Licensure.

The Commonwealth of Massachusetts

In the One Hundred and Ninetieth General Court
(2017-2018)

An Act protecting the privacy of consumer financial information.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. This bill shall be known and may be cited as the “Massachusetts Financial Information Privacy Act”

SECTION 2. The General Laws are hereby amended by inserting after chapter 93J the following new chapter:-

CHAPTER 93K.

Privacy of Consumer Financial Information.

Section 1. Whenever used in this chapter, the following terms, unless the context clearly indicates otherwise, shall have the following meanings:

"Affiliate" means any entity that controls, is controlled by, or is under common control with, another entity, but does not include a joint employee of the entity and the affiliate. A

franchisor, including any affiliate thereof, shall be deemed an affiliate of the franchisee for purposes of this division.

"Clear and conspicuous" means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information contained in the notice.

"Consumer" means an individual resident of this state, or that individual's legal representative, who obtains or has obtained from a financial institution a financial product or service to be used primarily for personal, family, or household purposes. For purposes of this division, an individual resident of this state is someone whose last known mailing address, other than an Armed Forces Post Office or Fleet Post Office address, as shown in the records of the financial institution, is located in this state. For purposes of this division, an individual is not a consumer of a financial institution solely because he or she is a participant or beneficiary of an employee benefit plan that a financial institution administers or sponsors, or for which the financial institution acts as a trustee, insurer, or fiduciary, covered under a group or blanket insurance policy or group annuity contract issued by the financial institution, a beneficiary in a workers' compensation plan, a beneficiary of a trust for which the financial institution is a trustee, or a person who has designated the financial institution as trustee for a trust, provided that the financial institution provides all required notices and rights required by this division to the plan sponsor, group or blanket insurance policyholder, or group annuity contract holder.

"Control" means ownership or power to vote 25 percent or more of the outstanding shares of any class of voting security of a company, acting through one or more persons, control in any manner over the election of a majority of the directors, or of individuals exercising similar functions, or the power to exercise, directly or indirectly, a controlling influence over the

management or policies of a company. However, for purposes of the application of the definition of control as it relates to credit unions, a credit union has a controlling influence over the management or policies of a credit union service organization (CUSO), as that term is defined by state or federal law or regulation, if the CUSO is at least 67 percent owned by credit unions. For purposes of the application of the definition of control to a financial institution subject to regulation by the United States Securities and Exchange Commission, a person who owns beneficially, either directly or through one or more controlled companies, more than 25 percent of the voting securities of a company is presumed to control the company, and a person who does not own more than 25 percent of the voting securities of a company is presumed not to control the company, and a presumption regarding control may be rebutted by evidence, but in the case of an investment company, the presumption shall continue until the United States Securities and Exchange Commission makes a decision to the contrary according to the procedures described in Section 2(a)(9) of the federal Investment Company Act of 1940.

"Financial institution" means any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 of the United States Code and doing business in this state. An institution that is not significantly engaged in financial activities is not a financial institution. The term "financial institution" does not include any institution that is primarily engaged in providing hardware, software, or interactive services, provided that it does not act as a debt collector, as defined in 15 U.S.C. Sec. 1692a, or engage in activities for which the institution is required to acquire a charter, license, or registration from a state or federal governmental banking, insurance, or securities agency. The term "financial institution" does not include the Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971 (12 U.S.C. Sec. 2001 et seq.), provided that the

entity does not sell or transfer nonpublic personal information to an affiliate or a nonaffiliated third party. The term "financial institution" does not include institutions chartered by Congress specifically to engage in a proposed or actual securitization, secondary market sale, including sales of servicing rights, or similar transactions related to a transaction of the consumer, as long as those institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party. The term "financial institution" does not include any provider of professional services, or any wholly owned affiliate thereof, that is prohibited by rules of professional ethics and applicable law from voluntarily disclosing confidential client information without the consent of the client.

"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 a financial activity under subsection (k) of Section 1843 of Title 12 of the United States Code (the United States Bank Holding Company Act of 1956). 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.

“Necessary to effect, administer, or enforce" means the following:

(1) The disclosure is required, or is a usual, appropriate, or acceptable method to carry out the transaction or the product or service business of which the transaction is a part, and record or service or maintain the consumer's account in the ordinary course of providing the financial service or financial product, or to administer or service benefits or claims relating to the transaction or the product or service business of which it is a part, and includes the following:

(i) Providing the consumer or the consumer's agent or broker with a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product.

(ii) The accrual or recognition of incentives, discounts, or bonuses associated with the transaction or communications to eligible existing consumers of the financial institution regarding the availability of those incentives, discounts, and bonuses that are provided by the financial institution or another party.

(iii) In the case of a financial institution that has issued a credit account bearing the name of a company primarily engaged in retail sales or a name proprietary to a company primarily engaged in retail sales, the financial institution providing the retailer with nonpublic personal information as follows:

(A) Providing the retailer, or licensees or contractors of the retailer that provide products or services in the name of the retailer and under a contract with the retailer, with the names and addresses of the consumers in whose name the account is held and a record of the purchases made using the credit account from a business establishment, including a Web site or catalog, bearing the brand name of the retailer.

(B) Where the credit account can only be used for transactions with the retailer or affiliates of that retailer that are also primarily engaged in retail sales, providing the retailer, or licensees or contractors of the retailer that provide products or services in the name of the retailer and under a contract with the retailer, with nonpublic personal information concerning the credit account, in connection with the offering or provision of the products or services of the retailer and those licensees or contractors.

(2) The disclosure is required or is one of the lawful or appropriate methods to enforce the rights of the financial institution or of other persons engaged in carrying out the financial transaction or providing the product or service.

(3) The disclosure is required, or is a usual, appropriate, or acceptable method for insurance underwriting or the placement of insurance products by licensed agents and brokers with authorized insurance companies at the consumer's request, for reinsurance, stop loss insurance, or excess loss insurance purposes, or for any of the following purposes as they relate to a consumer's insurance:

(i) Account administration.

(ii) Reporting, investigating, or preventing fraud or material misrepresentation.

(iii) Processing premium payments.

(iv) Processing insurance claims.

(v) Administering insurance benefits, including utilization review activities.

(vi) Participating in research projects.

(vii) As otherwise required or specifically permitted by federal or state law.

(4) The disclosure is required, or is a usual, appropriate, or acceptable method, in connection with the following:

(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.

(iii) The audit of debit, credit, or other payment information.

(5) The disclosure is required in a transaction covered by the federal Real Estate Settlement Procedures Act (12 U.S.C. Sec. 2601 et seq.) in order to offer settlement services prior to the close of escrow (as those services are defined in 12 U.S.C. Sec. 2602), provided that the nonpublic personal information is disclosed for the sole purpose of offering those settlement services and the nonpublic personal information disclosed is limited to that necessary to enable the financial institution to offer those settlement services in that transaction.

"Nonaffiliated third party" means any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the financial institution, but does not include a joint employee of that institution and a third party.

"Nonpublic personal information" means personally identifiable financial information provided by a consumer to a financial institution resulting from any transaction with the consumer or any service performed for the consumer or otherwise obtained by the financial institution. Nonpublic personal information does not include publicly available information that the financial institution has a reasonable basis to believe is lawfully made available to the general public from federal, state, or local government records, widely distributed media, or disclosures to the general public that are required to be made by federal, state, or local law. Nonpublic personal information shall include any list, description, or other grouping of consumers, and publicly available information pertaining to them, that is derived using any nonpublic personal information other than publicly available information, but shall not include any list, description,

or other grouping of consumers, and publicly available information pertaining to them, that is derived without using any nonpublic personal information.

"Personally identifiable financial information" means information that a consumer provides to a financial institution to obtain a product or service from the financial institution, about a consumer resulting from any transaction involving a product or service between the financial institution and a consumer, or that the financial institution otherwise obtains about a consumer in connection with providing a product or service to that consumer. Any personally identifiable information is financial if it was obtained by a financial institution in connection with providing a financial product or service to a consumer. Personally identifiable financial information includes all of the following:

(1) Information a consumer provides to a financial institution on an application to obtain a loan, credit card, or other financial product or service.

(2) Account balance information, payment history, overdraft history, and credit or debit card purchase information.

(3) The fact that an individual is or has been a consumer of a financial institution or has obtained a financial product or service from a financial institution.

(4) Any information about a 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.

(5) Any information that a consumer provides to a financial institution or that a financial institution or its agent otherwise obtains in connection with collecting on a loan or servicing a loan.

(6) Any personally identifiable financial information collected through an Internet cookie or an information collecting device from a Web server.

(7) Information from a consumer report.

"Widely distributed media" means media available to the general public and includes 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.

Section 2. Except as provided in sections 3, 6, and 7, a financial institution shall not sell, share, transfer, or otherwise disclose nonpublic personal information to or with any nonaffiliated third parties without the explicit prior consent of the consumer to whom the nonpublic personal information relates.

Section 3. (a) (1) A financial institution shall not disclose to, or share a consumer's nonpublic personal information with, any nonaffiliated third party as prohibited by section 2 unless the financial institution has obtained a consent acknowledgment from the consumer that complies with paragraph (2) that authorizes the financial institution to disclose or share the nonpublic personal information. Nothing in this section shall prohibit or otherwise apply to the disclosure of nonpublic personal information as allowed in section 7. A financial institution shall not discriminate against or deny an otherwise qualified consumer a financial product or a financial service because the consumer has not provided consent pursuant to this subsection and section 2 to authorize the financial institution to disclose or share nonpublic personal information pertaining to him or her with any nonaffiliated third party. Nothing in this section shall prohibit a financial institution from denying a consumer a financial product or service if the financial institution could not provide the product or service to a consumer without the consent to disclose

the consumer's nonpublic personal information required by this subsection and section 2 and the consumer has failed to provide consent. A financial institution shall not be liable for failing to offer products and services to a consumer solely because that consumer has failed to provide consent pursuant to this subsection and section 2 and the financial institution could not offer the product or service without the consent to disclose the consumer's nonpublic personal information required by this subsection and section 2, and the consumer has failed to provide consent. Nothing in this section is intended to prohibit a financial institution from offering incentives or discounts to elicit a specific response to the notice.

(2) A financial institution shall utilize a form, statement, or writing to obtain consent to disclose nonpublic personal information to nonaffiliated third parties as required by section 2 and this subsection. The form, statement, or writing shall meet all of the following criteria:

(i) the form, statement, or writing is a separate document, not attached to any other document.

(ii) the form, statement, or writing is dated and signed by the consumer.

(iii) the form, statement, or writing clearly and conspicuously discloses that by signing, the consumer is consenting to the disclosure to nonaffiliated third parties of nonpublic personal information pertaining to the consumer.

(iii) the form, statement, or writing clearly and conspicuously discloses:

(A) that the consent will remain in effect until revoked or modified by the consumer;

(B) that the consumer may revoke the consent at any time; and

(C) the procedure for the consumer to revoke consent.

(iv) the form, statement, or writing clearly and conspicuously informs the consumer that

(A) the financial institution will maintain the document or a true and correct copy;

(B) the consumer is entitled to a copy of the document upon request; and

(C) the consumer may want to make a copy of the document for the consumer's records.

(b) (1) A financial institution shall not disclose to, or share a consumer's nonpublic personal information with, an affiliate unless the financial institution has clearly and conspicuously notified the consumer annually in writing pursuant to subsection (d) that the nonpublic personal information may be disclosed to an affiliate of the financial institution and the consumer has not directed that the nonpublic personal information not be disclosed. A financial institution does not disclose information to, or share information with, its affiliate merely because information is maintained in common information systems or databases, and employees of the financial institution and its affiliate have access to those common information systems or databases, or a consumer accesses a Web site jointly operated or maintained under a common name by or on behalf of the financial institution and its affiliate, provided that where a consumer has exercised his or her right to prohibit disclosure pursuant to this division, nonpublic personal information is not further disclosed or used by an affiliate except as permitted by this division.

(2) Subsection (a) shall not prohibit the release of nonpublic personal information by a financial institution with whom the consumer has a relationship to a nonaffiliated financial institution for purposes of jointly offering a financial product or financial service pursuant to a written agreement with the financial institution that receives the nonpublic personal information provided that all of the following requirements are met:

(i) The financial product or service offered is a product or service of, and is provided by, at least one of the financial institutions that is a party to the written agreement.

(ii) The financial product or service is jointly offered, endorsed, or sponsored, and clearly and conspicuously identifies for the consumer the financial institutions that disclose and receive the disclosed nonpublic personal information.

(iii) The written agreement provides that the financial institution that receives that nonpublic personal information is required to maintain the confidentiality of the information and is prohibited from disclosing or using the information other than to carry out the joint offering or servicing of a financial product or financial service that is the subject of the written agreement.

(iv) The financial institution that releases the nonpublic personal information has complied with subsection (d) and the consumer has not directed that the nonpublic personal information not be disclosed.

(v) Notwithstanding this section, up until a year after the date this Act goes into effect, a financial institution may disclose nonpublic personal information to a nonaffiliated financial institution pursuant to a preexisting contract with the nonaffiliated financial institution, for purposes of offering a financial product or financial service, if that contract was entered into on or before the date this act goes into effect. Beginning one year after this Act goes into effect, no nonpublic personal information may be disclosed pursuant to that contract unless all the requirements of this subsection are met.

(3) Nothing in this subsection shall prohibit a financial institution from disclosing or sharing nonpublic personal information as otherwise specifically permitted by this division.

(4) A financial institution shall not discriminate against or deny an otherwise qualified consumer a financial product or a financial service because the consumer has directed pursuant to this subsection that nonpublic personal information pertaining to him or her not be disclosed. A financial institution shall not be required to offer or provide products or services offered through affiliated entities or jointly with nonaffiliated financial institutions pursuant to paragraph (2) where the consumer has directed that nonpublic personal information not be disclosed pursuant to this subsection and the financial institution could not offer or provide the products or services to the consumer without disclosure of the consumer's nonpublic personal information that the consumer has directed not be disclosed pursuant to this subsection. A financial institution shall not be liable for failing to offer or provide products or services offered through affiliated entities or jointly with nonaffiliated financial institutions pursuant to paragraph (2) solely because the consumer has directed that nonpublic personal information not be disclosed pursuant to this subsection and the financial institution could not offer or provide the products or services to the consumer without disclosure of the consumer's nonpublic personal information that the consumer has directed not be disclosed to affiliates pursuant to this subsection. Nothing in this section is intended to prohibit a financial institution from offering incentives or discounts to elicit a specific response to the notice set forth in this division. Nothing in this section shall prohibit the disclosure of nonpublic personal information allowed by section 7.

(5) The financial institution may, at its option, choose instead to comply with the requirements of subsection (a).

(c) Nothing in this division shall restrict or prohibit the sharing of nonpublic personal information between a financial institution and its wholly owned financial institution subsidiaries; among financial institutions that are each wholly owned by the same financial

institution; among financial institutions that are wholly owned by the same holding company; or among the insurance and management entities of a single insurance holding company system consisting of one or more reciprocal insurance exchanges which has a single corporation or its wholly owned subsidiaries providing management services to the reciprocal insurance exchanges, provided that in each case all of the following requirements are met:

(1) The financial institution disclosing the nonpublic personal information and the financial institution receiving it are regulated by the same functional regulator; provided, however, that financial institutions regulated by the Securities and Exchange Commission, the United States Department of Labor, or a state securities regulator shall be deemed to be regulated by the same functional regulator; and insurers admitted in this state to transact insurance and licensed to write insurance policies shall be deemed to be in compliance with this paragraph.

(2) The financial institution disclosing the nonpublic personal information and the financial institution receiving it are both principally engaged in the same line of business. For purposes of this subsection, "same line of business" shall be one and only one of the following:

(i) Insurance.

(ii) Banking.

(iii) Securities.

(3) The financial institution disclosing the nonpublic personal information and the financial institution receiving it share a common brand, excluding a brand consisting solely of a graphic element or symbol, within their trademark, service mark, or trade name, which is used to identify the source of the products and services provided. A wholly owned subsidiary shall

include a subsidiary wholly owned directly or wholly owned indirectly in a chain of wholly owned subsidiaries. Nothing in this subsection shall permit the disclosure by a financial institution of medical record information except in compliance with the requirements of this division, including the requirements set forth in subsections (a) and (b).

(d) (1) A form shall be sent by the financial institution to the consumer so that the consumer may make a decision and provide direction to the financial institution regarding the sharing of his or her nonpublic personal information; provided, however, that the form meets the following requirements:

(i) The form uses the following title ("IMPORTANT PRIVACY CHOICES FOR CONSUMERS") and the headers, if applicable, as follows: "Restrict Information Sharing With Companies We Own Or Control (Affiliates)" and "Restrict Information Sharing With Other Companies We Do Business With To Provide Financial Products And Services."

(ii) The titles and headers in the form are clearly and conspicuously displayed, and no text in the form is smaller than 10-point type.

(iii) The form is a separate document, except as provided by section 5.

(iv) The choice or choices pursuant to subsection (b) and section 6, if applicable, provided in the form are stated separately and may be selected by checking a box.

(v) The form is designed to call attention to the nature and significance of the information in the document.

(vi) The form presents information in clear and concise sentences, paragraphs, and sections.

(vii) The form uses short explanatory sentences (an average of 15-20 words) or bullet lists whenever possible.

(viii) The form avoids multiple negatives, legal terminology, and highly technical terminology whenever possible.

(ix) The form avoids explanations that are imprecise and readily subject to different interpretations.

(x) The form provides wide margins, ample line spacing and uses boldface or italics for key words.

(xi) The form is not more than one page.

(2) The office of consumer affairs and business regulation shall create a model notification form that financial institutions can use to notify consumers. The model form shall conform to the requirements laid out in subsection (d) paragraph (1). A financial institution shall be conclusively presumed to have satisfied the notice requirements of subsection (b) if it uses this model form.

(3) The consumer shall be provided a reasonable opportunity prior to disclosure of nonpublic personal information to direct that nonpublic personal information not be disclosed. A consumer may direct at any time that his or her nonpublic personal information not be disclosed. A financial institution shall comply with a consumer's directions concerning the sharing of his or her nonpublic personal information within 45 days of receipt by the financial institution. When a consumer directs that nonpublic personal information not be disclosed, that direction is in effect until otherwise stated by the consumer. A financial institution that has not provided a consumer

with annual notice pursuant to subsection (b) shall provide the consumer with a form that meets the requirements of this subsection, and shall allow 45 days to lapse from the date of providing the form in person or the postmark or other postal verification of mailing before disclosing nonpublic personal information pertaining to the consumer. Nothing in this subsection shall prohibit the disclosure of nonpublic personal information as allowed by subsection (c) or section 7.

(4) A financial institution may elect to comply with the requirements of subsection (a) with respect to disclosure of nonpublic personal information to an affiliate or with respect to nonpublic personal information disclosed pursuant to paragraph (2) of subsection (b), or subsection (c) of section 6.

(5) If a financial institution does not have a continuing relationship with a consumer other than the initial transaction in which the product or service is provided, no annual disclosure requirement exists pursuant to this section as long as the financial institution provides the consumer with the form required by this section at the time of the initial transaction. As used in this section, "annually" means at least once in any period of 12 consecutive months during which that relationship exists. The financial institution may define the 12-consecutive-month period, but shall apply it to the consumer on a consistent basis. If, for example, a financial institution defines the 12-consecutive-month period as a calendar year and provides the annual notice to theconsumer once in each calendar year, it complies with the requirement to send the notice annually.

(6) A financial institution with assets in excess of $25,000,000 shall include a self-addressed first class business reply return envelope with the notice. A financial institution with

assets of up to and including $25,000,000 shall include a self-addressed return envelope with the notice. In lieu of the first class business reply return envelope required by this paragraph, a financial institution may offer a self-addressed return envelope with the notice and at least two alternative cost-free means for consumers to communicate their privacy choices, such as calling a toll-free number, sending a facsimile to a toll-free telephone number, or using electronic means. A financial institution shall clearly and conspicuously disclose in the form required by this subsection the information necessary to direct the consumer on how to communicate his or her choices, including the toll-free or facsimile number or Web site address that may be used, if those means of communication are offered by the financial institution.

(7) A financial institution may provide a joint notice from it and one or more of its affiliates or other financial institutions, as identified in the notice, so long as the notice is accurate with respect to the financial institution and the affiliates and other financial institutions.

(e) Nothing in this division shall prohibit a financial institution from marketing its own products and services or the products and services of affiliates or nonaffiliated third parties to customers of the financial institution as long as:

(1) nonpublic personal information is not disclosed in connection with the delivery of the applicable marketing materials to those customers except as permitted by section 7, and

(2) in cases in which the applicable nonaffiliated third party may extrapolate nonpublic personal information about the consumer responding to those marketing materials, the applicable nonaffiliated third party has signed a contract with the financial institution under the terms of which:

(A) the nonaffiliated third party is prohibited from using that information for any purpose other than the purpose for which it was provided, as set forth in the contract, and

(B) the financial institution has the right by audit, inspections, or other means to verify the nonaffiliated third party's compliance with that contract.

Section 4. Except as otherwise provided in this division, an entity that receives nonpublic personal information from a financial institution under this division shall not disclose this information to any other entity, unless the disclosure would be lawful if made directly to the other entity by the financial institution. An entity that receives nonpublic personal information pursuant to any exception set forth in section 7 shall not use or disclose the information except in the ordinary course of business to carry out the activity covered by the exception under which the information was received.

Section 5. (a) Nothing in this division shall require a financial institution to provide a written notice to a consumer pursuant to section 3 if the financial institution does not disclose nonpublic personal information to any nonaffiliated third party or to any affiliate, except as allowed in this division.

(b) A notice provided to a member of a household pursuant to section 3 shall be considered notice to all members of that household unless that household contains another individual who also has a separate account with the financial institution.

(c) (1) The requirement to send a written notice to a consumer may be fulfilled by electronic means if the following requirements are met:

(i) The notice, and the manner in which it is sent, meets all of the requirements for notices that are required by law to be in writing, as set forth in section 101 of the federal Electronic Signatures in Global and National Commerce Act.

(ii) All other requirements applicable to the notice, as set forth in this division, are met, including, but not limited to, requirements concerning content, timing, form, and delivery. An electronic notice sent pursuant to this section is not required to include a return envelope.

(iii) The notice is delivered to the consumer in a form the consumer may keep.

(2) A notice that is made available to a consumer, and is not delivered to the consumer, does not satisfy the requirements of paragraph (1).

(3) Any electronic consumer reply to an electronic notice sent pursuant to this division is effective. A person that electronically sends a notice required by this division to a consumer may not by contract, or otherwise, eliminate the effectiveness of the consumer's electronic reply.

(4) This division modifies the provisions of section 101 of the federal Electronic Signatures in Global and National Commerce Act. However, it does not modify, limit, or supersede the provisions of subsection (c), (d), (e), (f), or (h) of section 101 of the federal Electronic Signatures in Global and National Commerce Act, nor does it authorize electronic delivery of any notice of the type described in subsection (b) of section 103 of that federal act.

Section 6. (a) When a financial institution and an organization or business entity that is not a financial institution ("affinity partner") have an agreement to issue a credit card in the name of the affinity partner ("affinity card"), the financial institution shall be permitted to disclose to the affinity partner in whose name the card is issued only the following information pertaining to

the financial institution's customers who are in receipt of the affinity card: (1) name, address, telephone number, and electronic mail address and (2) record of purchases made using the affinity card in a business establishment, including a Web site, bearing the brand name of the affinity partner.

(b) When a financial institution and an affinity partner have an agreement to issue a financial product or service, other than a credit card, on behalf of the affinity partner ("affinity financial product or service"), the financial institution shall be permitted to disclose to the affinity partner only the following information pertaining to the financial institution's customers who obtained the affinity financial product or service: name, address, telephone number, and electronic mail address.

(c) The disclosures specified in subsections (a) and (b) shall be permitted only if the following requirements are met:

(1) The financial institution has provided the consumer a notice meeting the requirements of subsection (d) of section 3, and the consumer has not directed that nonpublic personal information not be disclosed. A response to a notice meeting the requirements of subsection (d) directing the financial institution to not disclose nonpublic personal information to a nonaffiliated financial institution shall be deemed a direction to the financial institution to not disclose nonpublic personal information to an affinity partner, unless the form containing the notice provides the consumer with a separate choice for disclosure to affinity partners.

(2) The financial institution has a contractual agreement with the affinity partner that requires the affinity partner to maintain the confidentiality of the nonpublic personal information and prohibits affinity partners from using the information for any purposes other than verifying

membership, verifying the consumer's contact information, or offering the affinity partner's own products or services to the consumer.

(3) The customer list is not disclosed in any way that reveals or permits extrapolation of any additional nonpublic personal information about any customer on the list.

(4) If the affinity partner sends any message to any electronic mail addresses obtained pursuant to this section, the message shall include at least both of the following:

(i) The identity of the sender of the message.

(ii) A cost-free means for the recipient to notify the sender not to electronically mail any further message to the recipient.

(iii) Nothing in this section shall prohibit the disclosure of nonpublic personal information pursuant to section 7.

(iv) This section does not apply to credit cards issued in the name of an entity primarily engaged in retail sales or a name proprietary to a company primarily engaged in retail sales.

Section 7 . (a) This division shall not apply to information that is not personally identifiable to a particular person.

(b) Notwithstanding sections 2, 3, 5, and 6, a financial institution may release nonpublic personal information under the following circumstances:

(1) The nonpublic personal information is necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with servicing or processing a financial product or service requested or authorized by the consumer, or in

connection with maintaining or servicing the consumer's account with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of that entity, or in connection with a proposed or actual securitization or secondary market sale, including sales of servicing rights, or similar transactions related to a transaction of the consumer.

(2) The nonpublic personal information is released with the consent of or at the direction of the consumer.

(3) The nonpublic personal information is:

(i) Released to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction therein.

(ii) Released to protect against or prevent actual or potential fraud, identity theft, unauthorized transactions, claims, or other liability.

(iii) Released for required institutional risk control, or for resolving customer disputes or inquiries.

(iv) Released to persons holding a legal or beneficial interest relating to the consumer, including for purposes of debt collection.

(v) Released to persons acting in a fiduciary or representative capacity on behalf of the consumer.

(4) The nonpublic personal information is released to provide information to insurance rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the

financial institution, persons assessing the institution's compliance with industry standards, and the institution's attorneys, accountants, and auditors.

(5) The nonpublic personal information is released to the extent specifically required or specifically permitted under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978 (12 U.S.C. Sec. 3401 et seq.), to law enforcement agencies, including a federal functional regulator, the Secretary of the Treasury with respect to subchapter II of Chapter 53 of Title 31, and Chapter 2 of Title I of Public Law 91-508 (12 U.S.C. Secs. 1951-1959), or the Federal Trade Commission, and self-regulatory organizations, or for an investigation on a matter related to public safety.

(6) The nonpublic personal information is released in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of the business or unit.

(7) The nonpublic personal information is released to comply with federal, state, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, administrative, or regulatory investigation or subpoena or summons by federal, state, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law.

(8) When a financial institution is reporting a known or suspected instance of elder or dependent adult financial abuse or is cooperating with a local adult protective services agency investigation of known or suspected elder or dependent adult financial abuse.

(9) The nonpublic personal information is released to an affiliate or a nonaffiliated third party in order for the affiliate or nonaffiliated third party to perform business or professional services, such as printing, mailing services, data processing or analysis, or customer surveys, on behalf of the financial institution, provided that all of the following requirements are met:

(i) The services to be performed by the affiliate or nonaffiliated third party could lawfully be performed by the financial institution.

(ii) There is a written contract between the affiliate or nonaffiliated third party and the financial institution that prohibits the affiliate or nonaffiliated third party, as the case may be, from disclosing or using the nonpublic personal information other than to carry out the purpose for which the financial institution disclosed the information, as set forth in the written contract.

(iii) The nonpublic personal information provided to the affiliate or nonaffiliated third party is limited to that which is necessary for the affiliate or nonaffiliated third party to perform the services contracted for on behalf of the financial institution.

(iv) The financial institution does not receive any payment from or through the affiliate or nonaffiliated third party in connection with, or as a result of, the release of the nonpublic personal information.

(10) The nonpublic personal information is released to identify or locate missing and abducted children, witnesses, criminals and fugitives, parties to lawsuits, parents delinquent in child support payments, organ and bone marrow donors, pension fund beneficiaries, and missing heirs.

(11) The nonpublic personal information is released as required by Title III of the federal United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act; P.L. 107-56).

(12) The nonpublic personal information is released either to a consumer reporting agency pursuant to the Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.) or from a consumer report reported by a consumer reporting agency.

(13) The nonpublic personal information is released in connection with a written agreement between a consumer and a broker-dealer registered under the Securities Exchange Act of 1934 or an investment adviser registered under the Investment Advisers Act of 1940 to provide investment management services, portfolio advisory services, or financial planning, and the nonpublic personal information is released for the sole purpose of providing the products and services covered by that agreement.

(c) Nothing in this division is intended to change existing law relating to access by law enforcement agencies to information held by financial institutions.

Section 8. (a) An entity that negligently discloses or shares nonpublic personal information in violation of this division shall be liable, irrespective of the amount of damages suffered by the consumer as a result of that violation, for a civil penalty not to exceed two thousand five hundred dollars ($2,500) per violation. However, if the disclosure or sharing results in the release of nonpublic personal information of more than one individual, the total civil penalty awarded pursuant to this subsection shall not exceed five hundred thousand dollars ($500,000).

(b) An entity that knowingly and willfully obtains, discloses, shares, or uses nonpublic personal information in violation of this division shall be liable for a civil penalty not to exceed two thousand five hundred dollars ($2,500) per individual violation, irrespective of the amount of damages suffered by the consumer as a result of that violation.

(c) In determining the penalty to be assessed pursuant to a violation of this division, the court shall take into account the following factors:

(1) The total assets and net worth of the violating entity.

(2) The nature and seriousness of the violation.

(3) The persistence of the violation, including any attempts to correct the situation leading to the violation.

(4) The length of time over which the violation occurred.

(5) The number of times the entity has violated this division.

(6) The harm caused to consumers by the violation.

(7) The level of proceeds derived from the violation.

(8) The impact of possible penalties on the overall fiscal solvency of the violating entity.

(d) In the event a violation of this division results in the identity theft of a consumer, the civil penalties set forth in this section shall be doubled.

(e) The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the Commonwealth of Massachusetts in any court of competent jurisdiction by the Attorney General.

Section 10. Nothing in this section shall be construed as altering or annulling the authority of any department or agency of the state to regulate any financial institution subject to its jurisdiction.

Section 11. This section shall preempt and be exclusive of all local agency ordinances and regulations relating to the use and sharing of nonpublic personal information by financial institutions. This section shall apply both prospectively and retroactively.

Section 12. The provisions of this division shall be severable, and if any phrase, clause, sentence, or provision is declared to be invalid or is preempted by federal law or regulation, the validity of the remainder of this division shall not be affected thereby.

Section 13. This division shall become operative six months after the passage of this Act.