

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:	
<i>James B. Eldridge</i>	<i>Middlesex and Worcester</i>	
<i>Robert M. Koczera</i>	<i>11th Bristol</i>	<i>2/2/2017</i>
<i>James Arciero</i>	<i>2nd Middlesex</i>	<i>2/3/2017</i>

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:

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

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

5 CHAPTER 93K.

6 Privacy of Consumer Financial Information.

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

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

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

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

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

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

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

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

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

65 "Financial product or service" means any product or service that a financial holding
66 company could offer by engaging in an activity that is financial in nature or incidental to a
67 financial activity under subsection (k) of Section 1843 of Title 12 of the United States Code (the
68 United States Bank Holding Company Act of 1956). Financial service includes a financial
69 institution's evaluation or brokerage of information that the financial institution collects in
70 connection with a request or an application from a consumer for a financial product or service.

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

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

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

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

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

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

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

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

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

107 (i) Account administration.

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

109 (iii) Processing premium payments.

110 (iv) Processing insurance claims.

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

112 (vi) Participating in research projects.

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

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

116 (i) The authorization, settlement, billing, processing, clearing, transferring, reconciling, or
117 collection of amounts charged, debited, or otherwise paid using a debit, credit or other payment
118 card, check, or account number, or by other payment means.

119 (ii) The transfer of receivables, accounts, or interests therein.

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

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

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

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

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

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

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

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

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

156 (4) Any information about a financial institution's consumer if it is disclosed in a manner
157 that indicates that the individual is or has been the financial institution's consumer.

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

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

163 (7) Information from a consumer report.

164 "Widely distributed media" means media available to the general public and includes a
165 telephone book, a television or radio program, a newspaper, or a Web site that is available to the
166 general public on an unrestricted basis.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

284 (i) Insurance.

285 (ii) Banking.

286 (iii) Securities.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

333 with annual notice pursuant to subsection (b) shall provide the consumer with a form that meets
334 the requirements of this subsection, and shall allow 45 days to lapse from the date of providing
335 the form in person or the postmark or other postal verification of mailing before disclosing
336 nonpublic personal information pertaining to the consumer. Nothing in this subsection shall
337 prohibit the disclosure of nonpublic personal information as allowed by subsection (c) or section
338 7.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

466 (3) The nonpublic personal information is:

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

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

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

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

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

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

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

481 (5) The nonpublic personal information is released to the extent specifically required or
482 specifically permitted under other provisions of law and in accordance with the Right to
483 Financial Privacy Act of 1978 (12 U.S.C. Sec. 3401 et seq.), to law enforcement agencies,
484 including a federal functional regulator, the Secretary of the Treasury with respect to subchapter
485 II of Chapter 53 of Title 31, and Chapter 2 of Title I of Public Law 91-508 (12 U.S.C. Secs.
486 1951-1959), or the Federal Trade Commission, and self-regulatory organizations, or for an
487 investigation on a matter related to public safety.

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

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

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

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

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

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

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

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

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

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

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

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

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

534 Section 8. (a) An entity that negligently discloses or shares nonpublic personal
535 information in violation of this division shall be liable, irrespective of the amount of damages
536 suffered by the consumer as a result of that violation, for a civil penalty not to exceed two
537 thousand five hundred dollars (\$2,500) per violation. However, if the disclosure or sharing
538 results in the release of nonpublic personal information of more than one individual, the total
539 civil penalty awarded pursuant to this subsection shall not exceed five hundred thousand dollars
540 (\$500,000).

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

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

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

548 (2) The nature and seriousness of the violation.

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

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

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

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

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

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

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

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

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

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

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

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