SENATE DOCKET, NO. 1806 FILED ON: 1/21/2011

SENATE . . . . . No. 100

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 passage of the accompanying:

An Act protecting the privacy of consumer financial information.

PETITION OF:

NAME:	DISTRICT/ADDRESS:
James B. Eldridge	☐ *[District]* ☐
Jennifer E. Benson	*37th Middlesex*
Sonia Chang-Diaz	☐ *[District]* ☐
Carolyn C. Dykema	*8th Middlesex*
Karen E. Spilka	☐ *[District]* ☐

SENATE DOCKET, NO. 1806 FILED ON: 1/21/2011

SENATE . . . . . No. 100

By Mr. Eldridge, a petition (accompanied by bill, Senate, No. 100) of James B. Eldridge, Jennifer E. Benson, Sonia Chang-Diaz, Carolyn C. Dykema and others for legislation to protect the privacy of consumer financial information. Consumer Protection and Professional Licensure.

The Commonwealth of Massachusetts

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 93I the following new chapter:-

CHAPTER 93J

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

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
85 name of a company primarily engaged in retail sales or a name proprietary to a company
86 primarily engaged in retail sales, the financial institution providing the retailer with nonpublic
87 personal information as follows:

88 (A) Providing the retailer, or licensees or contractors of the retailer that provide
89 products or services in the name of the retailer and under a contract with the retailer, with the
90 names and addresses of the consumers in whose name the account is held and a record of the
91 purchases made using the credit account from a business establishment, including a Web site or
92 catalog, 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,
117 reconciling, or collection of amounts charged, debited, or otherwise paid using a debit, credit or
118 other payment 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

135 has a reasonable basis to believe is lawfully made available to the general public from
136 federal, state, or local government records, widely distributed media, or disclosures to the
137 general public that are required to be made by federal, state, or local law. Nonpublic personal
138 information shall include any list, description, or other grouping of consumers, and publicly
139 available information

140 pertaining to them, that is derived using any nonpublic personal information other than
141 publicly available information, but shall not include any list, description, or other grouping of
142 consumers, and publicly available information pertaining to them, that is derived without using
143 any nonpublic personal information.

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

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

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

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

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

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

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

165 (7) Information from a consumer report.

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

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

173 Section 3. (a) (1) A financial institution shall not disclose to, or share a consumer's
174 nonpublic personal information with, any nonaffiliated third party as prohibited by Section 2
175 unless the financial institution has obtained a consent acknowledgment from the consumer that
176 complies with paragraph (2) that authorizes the financial institution to disclose or share the
177 nonpublic personal information. Nothing in this section shall prohibit or otherwise apply to the
178 disclosure of nonpublic personal information as allowed in Section 7. A financial institution shall
179 not discriminate against or deny an otherwise qualified consumer a financial product or a
180 financial service because the consumer has not provided consent pursuant to this subsection and
181 Section 2 to authorize the financial institution to disclose or share nonpublic personal
182 information pertaining to him or her with any nonaffiliated third party. Nothing in this section
183 shall prohibit a financial institution from denying a consumer a financial product or service if the
184 financial institution could not provide the product or service to a consumer without the consent
185 to disclose the consumer's nonpublic personal information required by this subsection and
186 Section 2 and the consumer has failed to provide consent. A financial institution shall not be
187 liable for failing to offer products and services to a consumer solely because that consumer has
188 failed to provide consent pursuant to this subsection and Section 2 and the financial institution
189 could not offer the product or service without the consent to disclose the consumer's nonpublic
190 personal information required by this subsection and Section 2, and the consumer has failed to
191 provide consent. Nothing in this section is intended to prohibit a financial institution from
192 offering incentives or discounts to elicit a specific response to the notice.

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

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

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

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

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

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

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

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

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

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

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

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

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

227 (2) Subsection (a) shall not prohibit the release of nonpublic personal information by a
228 financial institution with whom the consumer has a relationship to a nonaffiliated financial

229 institution for purposes of jointly offering a financial product or financial service pursuant to a
230 written agreement with the financial institution that receives the nonpublic personal information
231 provided that all of the following requirements are met:

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

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

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

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

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

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

253 (4) A financial institution shall not discriminate against or deny an otherwise qualified
254 consumer a financial product or a financial service because the consumer has directed pursuant
255 to this subsection that nonpublic personal information pertaining to him or her not be disclosed.
256 A financial institution shall not be required to offer or provide products or services offered
257 through affiliated entities or jointly with nonaffiliated financial institutions pursuant to paragraph
258 (2) where 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 pursuant to this subsection. A financial
262 institution shall not be liable for failing to offer or provide products or services offered through
263 affiliated entities or jointly with nonaffiliated financial institutions pursuant to paragraph (2)

264 solely because the consumer has directed that nonpublic personal information not be
265 disclosed pursuant to this subsection and the financial institution could not offer or provide the
266 products or services to the consumer without disclosure of the consumer's nonpublic personal
267 information that the consumer has directed not be disclosed to affiliates pursuant to this
268 subsection. Nothing in this section is intended to prohibit a financial institution from offering
269 incentives or discounts to elicit a specific response to the notice set forth in this division. Nothing
270 in this section shall prohibit the disclosure of nonpublic personal information allowed by Section
271 7.

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

274 (c) Nothing in this division shall restrict or prohibit the sharing of nonpublic personal
275 information between a financial institution and its wholly owned financial institution
276 subsidiaries; among financial institutions that are each wholly owned by the same financial
277 institution; among financial institutions that are wholly owned by the same holding company; or
278 among the insurance and management entities of a single insurance holding company system
279 consisting of one or more reciprocal insurance exchanges which has a single corporation or its
280 wholly owned subsidiaries providing management services to the reciprocal insurance
281 exchanges, provided that in each case all of the following requirements are met:

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

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

291 (i) Insurance.

292 (ii) Banking.

293 (iii)Securities.

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

299 owned subsidiaries. Nothing in this subsection shall permit the disclosure by a financial
300 institution of medical record information except in compliance with the requirements of this
301 division, including the requirements set forth in subsections (a) and (b).

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

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

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

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

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

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

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

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

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

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

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

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

328 (2) The Office of Consumer Affairs and Business Regulation shall create a model
329 notification form that financial institutions can use to notify consumers. The model form shall
330 conform to the requirements laid out in subsection (d) paragraph (1). A financial institution shall

331 be conclusively presumed to have satisfied the notice requirements of subsection (b) if it uses
332 this model form.

333 (3) The consumer shall be provided a reasonable opportunity prior to disclosure of
334 nonpublic personal information to direct that nonpublic personal information not be disclosed. A
335 consumer may direct at any time that his or her nonpublic personal information not be disclosed.
336 A financial institution shall comply with a consumer's directions concerning the sharing of his or
337 her nonpublic personal information within 45 days of receipt by the financial institution.

338 When a consumer directs that nonpublic personal information not be disclosed, that
339 direction is in effect until otherwise stated by the consumer. A financial institution that has not
340 provided a consumer with annual notice pursuant to subsection (b) shall provide the consumer
341 with a form that meets the requirements of this subsection, and shall allow 45 days to lapse from
342 the date of providing the form in person or the postmark or other postal verification of mailing
343 before disclosing nonpublic personal information pertaining to the consumer. Nothing in this
344 subsection shall prohibit the disclosure of nonpublic personal information as allowed by
345 subsection (c) or Section 7.

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

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

358 consumer once in each calendar year, it complies with the requirement to send the notice
359 annually.

360 (6) A financial institution with assets in excess of $25,000,000 shall include a self-
361 addressed first class business reply return envelope with the notice. A financial institution with
362 assets of up to and including $25,000,000 shall include a self-addressed return envelope with the
363 notice. In lieu of the first class business reply return envelope required by this paragraph, a
364 financial institution may offer a self-addressed return envelope with the notice and at least two
365 alternative cost-free means for consumers to communicate their privacy choices, such as calling
366 a toll-free number, sending a facsimile to a toll-free telephone number, or using electronic
367 means. A financial institution shall clearly and conspicuously disclose in the form required by

368 this subsection the information necessary to direct the consumer on how to communicate his or
369 her choices, including the toll-free or facsimile number or Web site address that may be used, if
370 those means of communication are offered by the financial institution.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

420 Section 6. (a) When a financial institution and an organization or business entity that is
421 not a financial institution ("affinity partner") have an agreement to issue a credit card in the name
422 of the affinity partner ("affinity card"), the financial institution shall be permitted to disclose to
423 the affinity partner in whose name the card is issued only the following information pertaining to
424 the financial institution's customers who are in receipt of the affinity card: (1) name, address,
425 telephone number, and electronic mail address and (2) record of purchases made using the
426 affinity card in a business establishment, including a Web site, bearing the brand name of the
427 affinity partner.

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

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

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

443 (2) The financial institution has a contractual agreement with the affinity partner that
444 requires the affinity partner to maintain the confidentiality of the nonpublic personal information
445 and prohibits affinity partners from using the information for any purposes other than verifying
446 membership, verifying the consumer's contact information, or offering the affinity partner's own
447 products or services to the consumer.

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

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

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

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

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

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

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

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

464 (1) The nonpublic personal information is necessary to effect, administer, or enforce a
465 transaction requested or authorized by the consumer, or in connection with servicing or
466 processing a financial product or service requested or authorized by the consumer, or in
467 connection with maintaining or servicing the consumer's account with the financial institution, or
468 with another entity as part of a private label credit card program or other extension of credit on
469 behalf of that entity, or in connection with a proposed or actual securitization or secondary

470 market sale, including sales of servicing rights, or similar transactions related to a transaction of
471 the consumer.

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

474 (3) The nonpublic personal information is:

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

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

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

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

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

485 (4) The nonpublic personal information is released to provide information to insurance
486 rate advisory organizations, guaranty funds or agencies, applicable rating agencies of the
487 financial institution, persons assessing the institution's compliance with industry standards, and
488 the institution's attorneys, accountants, and auditors.

489 (5) The nonpublic personal information is released to the extent specifically required or
490 specifically permitted under other provisions of law and in accordance with the Right to
491 Financial Privacy Act of 1978 (12 U.S.C. Sec. 3401 et seq.), to law enforcement agencies,
492 including a federal functional regulator, the Secretary of the Treasury with respect to subchapter
493 II of Chapter 53 of Title 31, and Chapter 2 of Title I of Public Law 91-508 (12 U.S.C. Secs.
494 1951-1959), or the Federal Trade Commission, and self-regulatory organizations, or for an
495 investigation on a matter related to public safety.

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

499 (7) The nonpublic personal information is released to comply with federal, state, or local
500 laws,

501 rules, and other applicable legal requirements; to comply with a properly authorized civil,
502 criminal, administrative, or regulatory investigation or subpoena or summons by federal, state, or

503 local authorities; or to respond to judicial process or government regulatory authorities having
504 jurisdiction over the financial institution for examination, compliance, or other purposes as
505 authorized by law.

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

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

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

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

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

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

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

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

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

535 (13) The nonpublic personal information is released in connection with a written
536 agreement between a consumer and a broker-dealer registered under the Securities Exchange Act

537 of 1934 or an investment adviser registered under the Investment Advisers Act of 1940 to
538 provide investment management services, portfolio advisory services, or financial planning, and
539 the nonpublic personal information is released for the sole purpose of providing the products and
540 services covered by that agreement.

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

543 Section 8. (a) An entity that negligently discloses or shares nonpublic personal
544 information in violation of this division shall be liable, irrespective of the amount of damages
545 suffered by the consumer as a result of that violation, for a civil penalty not to exceed two
546 thousand five hundred dollars ($2,500) per violation. However, if the disclosure or sharing
547 results in the release of nonpublic personal information of more than one individual, the total
548 civil penalty awarded pursuant to this subsection shall not exceed five hundred thousand dollars
549 ($500,000).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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