

**SENATE . . . . . No. 96**

---

**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>Kay Khan</i>	<i>11th Middlesex</i>
<i>Thomas P. Conroy</i>	<i>13th Middlesex</i>
<i>Sonia Chang-Diaz</i>	<i>Second Suffolk</i>
<i>Karen E. Spilka</i>	<i>Second Middlesex and Norfolk</i>
<i>Antonio F. D. Cabral</i>	<i>13th Bristol</i>
<i>Jennifer E. Benson</i>	<i>37th Middlesex</i>

**SENATE . . . . . No. 96**

---

By Mr. Eldridge, a petition (accompanied by bill, Senate, No. 96) of James B. Eldridge, Robert M. Koczera, Kay Khan, Thomas P. Conroy and other members of the General Court for legislation to protect the privacy of consumer financial information. Consumer Protection and Professional Licensure.

---

[SIMILAR MATTER FILED IN PREVIOUS SESSION  
SEE SENATE, NO. 100 OF 2011-2012.]

**The Commonwealth of Massachusetts**

—————  
**In the Year Two Thousand Thirteen**  
—————

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 93I the  
4 following new chapter:-

5 CHAPTER 93J.

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  
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, reconciling,  
117 or collection of amounts charged, debited, or otherwise paid using a debit, credit or other  
118 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 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

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

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

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

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

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

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

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

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

164 (7) Information from a consumer report.

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

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

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

190 Nothing in this section is intended to prohibit a financial institution from offering incentives or  
191 discounts to elicit a specific response to the notice.

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

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

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

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

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

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

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

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

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

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

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

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

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



222 consumer has exercised his or her right to prohibit disclosure pursuant to this division, nonpublic  
223 personal information is not further disclosed or used by an affiliate except as permitted by this  
224 division.

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

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

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

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

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

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

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

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

257 pursuant to this subsection and the financial institution could not offer or provide the products or  
258 services to the consumer without disclosure of the consumer's nonpublic personal information  
259 that the consumer has directed not be disclosed pursuant to this subsection. A financial  
260 institution shall not be liable for failing to offer or provide products or services offered through  
261 affiliated entities or jointly with nonaffiliated financial institutions pursuant to paragraph (2)  
262 solely because the consumer has directed that nonpublic personal information not be disclosed  
263 pursuant to this subsection and the financial institution could not offer or provide the products or  
264 services to the consumer without disclosure of the consumer's nonpublic personal information  
265 that the consumer has directed not be disclosed to affiliates pursuant to this subsection. Nothing  
266 in this section is intended to prohibit a financial institution from offering incentives or discounts  
267 to elicit a specific response to the notice set forth in this division. Nothing in this section shall  
268 prohibit the disclosure of nonpublic personal information allowed by section 7.

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

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

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

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

288 (i) Insurance.

289 (ii) Banking.

290 (iii) Securities.

291 (3) The financial institution disclosing the nonpublic personal information and the  
292 financial institution receiving it share a common brand, excluding a brand consisting solely of a  
293 graphic element or symbol, within their trademark, service mark, or trade name, which is used to  
294 identify the source of the products and services provided. A wholly owned subsidiary shall  
295 include a subsidiary wholly owned directly or wholly owned indirectly in a chain of wholly  
296 owned subsidiaries. Nothing in this subsection shall permit the disclosure by a financial  
297 institution of medical record information except in compliance with the requirements of this  
298 division, including the requirements set forth in subsections (a) and (b).

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

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

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

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

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

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

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

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

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

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

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

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

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

330 (3) The consumer shall be provided a reasonable opportunity prior to disclosure of  
331 nonpublic personal information to direct that nonpublic personal information not be disclosed. A  
332 consumer may direct at any time that his or her nonpublic personal information not be disclosed.  
333 A financial institution shall comply with a consumer's directions concerning the sharing of his or  
334 her nonpublic personal information within 45 days of receipt by the financial institution. When a  
335 consumer directs that nonpublic personal information not be disclosed, that direction is in effect  
336 until otherwise stated by the consumer. A financial institution that has not provided a consumer  
337 with annual notice pursuant to subsection (b) shall provide the consumer with a form that meets  
338 the requirements of this subsection, and shall allow 45 days to lapse from the date of providing  
339 the form in person or the postmark or other postal verification of mailing before disclosing  
340 nonpublic personal information pertaining to the consumer. Nothing in this subsection shall  
341 prohibit the disclosure of nonpublic personal information as allowed by subsection (c) or section  
342 7.

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

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

357 (6) A financial institution with assets in excess of \$25,000,000 shall include a self-  
358 addressed first class business reply return envelope with the notice. A financial institution with  
359 assets of up to and including \$25,000,000 shall include a self-addressed return envelope with the  
360 notice. In lieu of the first class business reply return envelope required by this paragraph, a

361 financial institution may offer a self-addressed return envelope with the notice and at least two  
362 alternative cost-free means for consumers to communicate their privacy choices, such as calling  
363 a toll-free number, sending a facsimile to a toll-free telephone number, or using electronic  
364 means. A financial institution shall clearly and conspicuously disclose in the form required by  
365 this subsection the information necessary to direct the consumer on how to communicate his or  
366 her choices, including the toll-free or facsimile number or Web site address that may be used, if  
367 those means of communication are offered by the financial institution.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

425 (b) When a financial institution and an affinity partner have an agreement to issue a  
426 financial product or service, other than a credit card, on behalf of the affinity partner ("affinity  
427 financial product or service"), the financial institution shall be permitted to disclose to the  
428 affinity partner only the following information pertaining to the financial institution's customers

429 who obtained the affinity financial product or service: name, address, telephone number, and  
430 electronic mail address.

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

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

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

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

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

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

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

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

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

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

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

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

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

471 (3) The nonpublic personal information is:

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

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

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

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

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

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

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



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

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

498 rules, and other applicable legal requirements; to comply with a properly authorized civil,  
499 criminal, administrative, or regulatory investigation or subpoena or summons by federal, state, or  
500 local authorities; or to respond to judicial process or government regulatory authorities having  
501 jurisdiction over the financial institution for examination, compliance, or other purposes as  
502 authorized by law.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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