

**SENATE . . . . . No. 869**

The Commonwealth of Massachusetts

PRESENTED BY:

***Karen E. Spilka***

*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 to protect the commonwealth's residents from identity theft.

PETITION OF:

NAME:	DISTRICT/ADDRESS:
<i>Karen E. Spilka</i>	
<i>Theodore C. Speliotis</i>	<i>13th Essex</i>
<i>Thomas P. Kennedy</i>	
<i>Michael J. Finn</i>	<i>6th Hampden</i>
<i>Kate Hogan</i>	<i>3rd Middlesex</i>
<i>Carolyn C. Dykema</i>	<i>8th Middlesex</i>
<i>Benjamin Swan</i>	<i>11th Hampden</i>
<i>Denise Provost</i>	<i>27th Middlesex</i>
<i>James M. Cantwell</i>	<i>4th Plymouth</i>
<i>Sal N. DiDomenico</i>	<i>Middlesex, Suffolk, and Essex</i>
<i>Robert M. Koczera</i>	<i>11th Bristol</i>
<i>David Paul Linsky</i>	<i>5th Middlesex</i>
<i>Cory Atkins</i>	<i>14th Middlesex</i>
<i>James B. Eldridge</i>	

**SENATE . . . . . No. 869**

---

By Ms. Spilka, a petition (accompanied by bill, Senate, No. 869) of Karen E. Spilka, Theodore C. Speliotis, Thomas P. Kennedy, Michael J. Finn and other members of the General Court for legislation to protect the Commonwealth's residents from identity theft. The Judiciary.

---

The Commonwealth of Massachusetts

—————  
**In the Year Two Thousand Eleven**  
—————

An act to protect the commonwealth's residents from identity theft.

*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. Section 37E of chapter 266 of the General Laws, as appearing in  
2 the 2008 Official Edition, is hereby amended by inserting before the definition “Harass” the  
3 following definition:- “Law enforcement agency”, any law enforcement organizations of the  
4 Commonwealth, or any of its political subdivisions. “Direct victim”, any person or entity whose  
5 identity has been transferred, used, or possessed in violation of this section.

6                   SECTION 2. Section 37E of chapter 266 of the General Laws, is hereby  
7 amended by inserting after the definition “Harass” the following definition:- “Identity theft  
8 passport”, a card or certificate issued by the attorney general that verifies the identity of the  
9 person who is a victim of identity theft or identity fraud. “Identity theft report”, a police incident  
10 report filed with a law enforcement agency containing specific details of an identity theft.  
11 “Indirect victim”, a corporation that incurs loss or harm as a result of a crime, a government  
12 entity that incurs loss or harm as a result of a crime, family members, guardians, custodians of a

13 minor, incompetent, incapacitated, or deceased persons that incurs loss or harm as a result of a  
14 crime, but not the person charged with or alleged to have committed the crime.

15           SECTION 3. Subsection (d) of section 37E of chapter 266 of the General Laws  
16 is hereby amended by inserting after the word “fees.” the following clause:- Upon written  
17 request by the victim, or by the prosecutor, the court shall provide to the victim, without cost: (1)  
18 a certified copy of the complaint filed in the matter; (2) the judgment of conviction; and (3) an  
19 order setting forth the facts and circumstances of the offense.

20           SECTION 4. Section 37E of chapter 266 of the General Laws is hereby  
21 amended by striking out subsection (e) and inserting in place thereof the following subsection:-  
22 (e) A person who has learned, or reasonably suspects that the person’s personal identifying  
23 information has been unlawfully obtained or used by another, may initiate a law enforcement  
24 investigation by contacting the local law enforcement that has jurisdiction over the person’s  
25 residence. A law enforcement officer shall accept an identity theft report from such victim and  
26 shall provide a copy to such victim, within 24 hours. Such police incident reports may be filed in  
27 any county where a victim resides or has a place of business, or in any county where the breach  
28 of security occurred, in whole or in part. The local law enforcement agency with whom the  
29 victim filed the initial complaint under this section shall begin an investigation of the facts, and  
30 shall, if the suspect resides in another jurisdiction, or if the suspected crime was committed in a  
31 different jurisdiction, or if information pertaining to the crime exists in another jurisdiction,  
32 notify the law enforcement agency in that jurisdiction of the matter.

33           SECTION 5. Section 37E of chapter 266 of the General Laws is hereby  
34 amended by inserting after subsection (e) the following subsections:- (f) (1) The department of

35 state police may initiate investigations and enforce this section throughout the Commonwealth  
36 without regard to any limitation otherwise applicable to the department's activities in a  
37 municipality or other political subdivision. The authority granted in this subsection may be  
38 exercised only in accordance with regulations that the department of state police adopts. (2) A  
39 law enforcement officer of a municipality or county may investigate violations of this section  
40 throughout the Commonwealth without any limitation as to jurisdiction and to the same extent as  
41 a law enforcement officer of the department of state police. The authority granted in this  
42 subsection may be exercised only if an act related to the crime was committed in the  
43 investigating law enforcement agency's jurisdiction or if the complaining witness resides, or has  
44 a principal place of business, in the investigating law enforcement agency's jurisdiction. (3) A  
45 law enforcement officer may arrest, without a warrant, any person he has probable cause to  
46 believe has committed the offense of identity fraud as defined in this section. (g) If action is  
47 taken under the authority granted in subsection (f) of this section, notification of an investigation:  
48 (1) in a municipal corporation, shall be made to the chief of police or designee of the chief of  
49 police; (2) in Boston, shall be made to the Police Commissioner or the Police Commissioner's  
50 designee; and (3) on property owned, leased, or operated by or under the control of the  
51 Massachusetts Bay Transportation Authority or the Massachusetts Port Authority, shall be made  
52 to the respective chief of police or the chief's designee. (h) (1) A district attorney or the attorney  
53 general may investigate and prosecute a violation of this section or a violation of any crime  
54 based on the act establishing a violation of this section. (i) In any criminal proceeding brought  
55 under this section, the crime is considered to be committed in the municipality: (1) where the  
56 direct victim, or indirect victim resides or has a place of business; (2) where the perpetrator  
57 resides; (3) where any part of the violation occurred, regardless of whether the defendant was

58 ever actually present in that municipality; or (4) in any other municipality instrumental to the  
59 completion of the offense, regardless of whether the defendant was ever physically present in  
60 that municipality. (j) In addition to the criminal penalties in subsections (d), of this section, any  
61 person who commits an act made unlawful by this section shall be liable to the person to whom  
62 the identifying information belonged, or the entity that suffered financial loss, for civil damages.  
63 (1) A victim under this section may bring an action in the superior court of her county of  
64 residence, or any county in which any part of the act took place, regardless of whether the person  
65 who committed the violation was ever physically present in that municipality. (2) The victim  
66 may institute a civil action to: (i) Enjoin and restrain future acts that would constitute a violation  
67 of this section; (ii) Recover \$5000 for each incident, or 3 times actual damages, whichever is  
68 greater; (iii) Recover reasonable attorneys' fees and costs; and (iv) Additional relief the court  
69 deems necessary. (3) A financial institution, insurance company, or business that suffers direct  
70 financial loss as a result of the offense may bring an action under this section and shall also be  
71 entitled to damages, but damages to natural persons shall be fully satisfied prior to any payment  
72 to a financial institution, insurance company, bonding association or business. (4) If the  
73 identifying information of a deceased person is used in a manner made unlawful by this section,  
74 or any other general or special law, the deceased person's estate shall have the right to recover  
75 damages pursuant to subsection (g) of this section. (5) No action under this section shall be  
76 brought but within five years from the date when the violation is discovered or, in the exercise of  
77 reasonable care, should have been discovered. (6) Civil action under this section does not depend  
78 on whether or not a criminal prosecution has been, or will be, instituted under this section for the  
79 acts which are the subject of the civil action. (7) A final judgment rendered in favor of the  
80 Commonwealth in any criminal proceeding shall estop the defendant from denying the same

81 conduct in any civil action brought pursuant to this section. (k) (1) A natural person who has,  
82 under this section, filed, with a law enforcement agency, a police report alleging identity theft  
83 under this section, may apply for an identity theft passport through any law enforcement agency,  
84 or directly through the attorney general. A law enforcement agency that receives an application  
85 for an identity theft passport shall submit the application and a copy of the identity theft report to  
86 the attorney general for processing and issuance of an identity theft passport. The attorney  
87 general, in cooperation with any law enforcement agency in the Commonwealth, may issue an  
88 identity theft passport to a person who is a victim of identity theft in this Commonwealth and  
89 who has filed a police report citing that such person is a victim of a violation of this chapter. This  
90 passport shall be in the form of a card or certificate, and must include photo identification. (2)  
91 The attorney general shall perform a background check on the identity theft victim before issuing  
92 an identity theft passport under this section. (3) An identity theft victim who has been issued an  
93 identity theft passport under this section may present this identity theft passport to: (i) a law  
94 enforcement agency to help prevent the arrest or detention of the person for an offense  
95 committed by another using the person's personal identifying information; or (ii) any of the  
96 victim's creditors to aid in the investigation of: (A) a fraudulent account that was opened in the  
97 person's name; or (B) a fraudulent charge that is made against an account of the person. (iii) A  
98 consumer reporting agency, as defined in § 603(f) of the federal Fair Credit Reporting Act (15  
99 U.S.C. § 1681a(f)), to expedite removal of accounts opened fraudulently by another and  
100 correcting credit report information. (4) A law enforcement agency or creditor that is presented  
101 with an identity theft passport under subsections (3)(i) or (3)(ii) of this section has sole discretion  
102 to accept or reject the identity theft passport. The consumer reporting agency must accept the  
103 passport as an official notice of a dispute and must include notice of the dispute in all future

104 reports that contain disputed information caused by the identity fraud. (5) An application for an  
105 identity theft passport submitted under this section, including any supporting documentation: (i)  
106 is not a public record; and (ii) may not be released except to a law enforcement agency in any  
107 state. (6) The attorney general shall adopt regulations to carry out the provisions of this section.  
108 The regulations must include a procedure by which the Office of the attorney general is  
109 reasonably assured that an identity theft passport applicant has an identity fraud claim that is  
110 legitimate and adequately substantiated.

111                   SECTION 6. Chapter 266 of the General Laws is hereby amended by inserting  
112 after section 37E the following section:- Section 37F. (a) For purpose of this section, the  
113 following words and terms shall have the following meanings:- "Advertisement", means a  
114 communication, the primary purpose of which is the commercial promotion of a commercial  
115 product or service, including content on an Internet Web site operated for a commercial purpose.  
116 "Authorized user", with respect to a computer, means a person who owns or is authorized by the  
117 owner or lessee to use the computer. An "authorized user" does not include a person or entity  
118 that has obtained authorization to use the computer solely through the use of an end user license  
119 agreement. "Computer or Internet settings", security or other settings that protect information  
120 about the authorized user, any page that appears when an authorized user launches an Internet  
121 browser or similar software program used to access and navigate the Internet, the default  
122 provider or Web proxy the authorized user uses to access or search the Internet, the authorized  
123 user's list of bookmarks used to access Web pages. "Computer software", a sequence of  
124 instructions written in any programming language that is executed on a computer. "Computer  
125 virus" means a computer program or other set of instructions that is designed to degrade the  
126 performance of or disable a computer or computer network and is designed to have the ability to

127 replicate itself on other computers or computer networks without the authorization of the owners  
128 of those computers or computer networks. "Consumer" means an individual who resides in this  
129 state and who uses the computer in question primarily for personal, family, or household  
130 purposes. "Damage" means any significant impairment to the integrity or availability of data,  
131 software, a system, or information. "Execute," when used with respect to computer software,  
132 means the performance of the functions or the carrying out of the instructions of the computer  
133 software. "Intentionally deceptive," by means of an intentionally and materially false or  
134 fraudulent statement, by means of a statement or description that intentionally omits or  
135 misrepresents material information in order to deceive the consumer, by means of an intentional  
136 and material failure to provide any notice to an authorized user regarding the download or  
137 installation of software in order to deceive the consumer. "Internet" means the global  
138 information system that is logically linked together by a globally unique address space based on  
139 the Internet Protocol (IP), or its subsequent extensions, and that is able to support  
140 communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, or its  
141 subsequent extensions, or other IP-compatible protocols, and that provides, uses, or makes  
142 accessible, either publicly or privately, high level services layered on the communications and  
143 related infrastructure described in this subdivision. "Payment card", a credit card, debit card, or  
144 any other card that is issued to an authorized user and that allows the user to obtain, purchase, or  
145 receive goods, services, money, or anything else of value. "Person", any natural person, business,  
146 or state or local agency or political subdivision. "Personally identifiable information", any name  
147 or number that may be used, alone or in conjunction with any other information, to assume the  
148 identity of an individual, including any name, address, telephone number, driver's license  
149 number, social security number, place of employment, employee identification number, mother's

150 maiden name, demand deposit account number, savings account number, credit card number or  
151 computer password identification. “Reencoder”, an electronic device that places encoded  
152 information from the magnetic strip or stripe of a payment card on to the magnetic strip or stripe  
153 of a payment card on to the magnetic strip or stripe of a different payment card. “Scanning  
154 device”, a scanner, reader, or any other electronic device that is used to access, read, scan,  
155 obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic  
156 strip or stripe of a payment card. “Skimming device”, a machine or instrument used to  
157 deceptively access, read, scan, obtain, memorize, or store, temporarily or permanently, payment  
158 card information or a person’s personal identification number, used in an otherwise legitimate  
159 transaction. (b) Any person who is not an authorized user shall not: (1) Transmit computer  
160 software to the authorized user’s computer with actual knowledge, or with conscious avoidance  
161 of actual knowledge, and to use such software, through intentionally deceptive means, to: (i)  
162 collect personally identifiable information, or collect information that meets any of the following  
163 criteria: (A) All keystrokes made by an authorized user who uses the computer and transfer that  
164 information from the computer to another person; (B) The Internet sites visited by an authorized  
165 user. (ii) modify computer or Internet settings; (iii) prevent an authorized user’s reasonable  
166 efforts to block installation, or execution of, or to disable, software, by: (A) falsely representing  
167 that software has been disabled. (B) causing software that the authorized user has properly  
168 removed or disabled to automatically reinstall or reactivate on the computer without the  
169 authorization of an authorized user; (C) presenting the authorized user with an option to decline  
170 installation of software with knowledge that, when the option is selected by the authorized user,  
171 the installation nevertheless proceeds. (iv) remove, disable, or render inoperative security,  
172 antispyware or antivirus computer software; (v) take control, through intentionally deceptive

173 means, of the consumer's computer; (vi) deceptively install, and execute, on the computer one or  
174 more additional computer software components with the intent of causing an authorized user to  
175 use the components in a way that violates any other provision of this section; (vii) access or use  
176 the consumer's modem or Internet service for the purpose of causing damage to the consumer's  
177 computer or causing an authorized user to incur unauthorized financial charges; (viii) use the  
178 consumer's computer as part of an activity performed by a group of computers for the purpose of  
179 causing damage to another computer, including launching a denial of service attack; (ix) open  
180 multiple, sequential, stand-alone advertisements in the consumer's Internet browser, without the  
181 authorization of an authorized user, and with knowledge that a reasonable computer user cannot  
182 close the advertisements without turning off the computer or closing the consumer's Internet  
183 browser; (2) By means of an Internet site, electronic mail message, or otherwise through use of  
184 the Internet, to solicit, request, or take action to induce another person to provide identifying  
185 information by representing itself to be a business without the authority or approval of the  
186 business. (c) No person shall knowingly, willfully, and with the intent to defraud, possess or use:  
187 (1) a scanning device to access, read, obtain, memorize or store, temporarily or permanently,  
188 information encoded on the magnetic strip or stripe of a payment card without the permission of  
189 the authorized user of the payment card; (2) a reencoder to place encoded information on the  
190 magnetic strip or stripe of a payment card or any electronic medium that allows an authorized  
191 transaction to occur, without the permission of the authorized user of the payment card from  
192 which the information is being reencoded; (3) a skimming device, or a camera, to obtain the  
193 account number or PIN of a payment card or any electronic medium that allows an authorized  
194 transaction to occur, without the permission of the authorized user of the payment card from  
195 which the information is being skimmed. (d) Any scanning device or reencoder or skimming

196 device described in this section owned by the defendant and possessed or used in violation of  
197 subsection (c) may be seized and be destroyed as contraband by law enforcement officials of the  
198 jurisdiction in which the scanning device or reencoder or skimming device was seized. (e) Any  
199 computer, computer system, computer network, or any software or data, owned by the defendant,  
200 which is used during the commission of any public offense described in this section, or any  
201 computer, owned by the defendant, which is used as a repository for the storage of software or  
202 data illegally obtained in violation of this section shall be subject to forfeiture. (f) Nothing in this  
203 section shall apply to any monitoring of, or interaction with, a subscriber's Internet or other  
204 network connection or service, or a protected computer, by a telecommunications carrier, cable  
205 operator, computer hardware or software provider, or provider of information service or  
206 interactive computer service for network or computer security purposes, diagnostics, technical  
207 support, repair, authorized updates of software or system firmware, authorized remote system  
208 management, or detection or prevention of the unauthorized use of or fraudulent or other illegal  
209 activities in connection with a network, service, or computer software, including scanning for  
210 and removing software proscribed under this chapter. (g) Any person who violates this section  
211 shall be guilty of a misdemeanor, punishable by a term in a county jail or house of correction not  
212 to exceed 1 year, or a fine of \$1,000, or both the imprisonment and fine. (h) Any person who  
213 violates this section and sells, distributes, or uses such information shall be guilty of a felony and  
214 punished by a fine of not more than \$5,000 or imprisonment in a state prison for not more than 2  
215 1/2 years, or by both such fine and imprisonment. (i) The attorney general may bring an action  
216 against a person who committed a violation under this section to enjoin further violations,  
217 recover a civil penalty of up to \$2500 per violation, or both. (j) Any person who is adversely  
218 affected by a violation of this section may bring an action to enjoin further violations, or recover

219 the greater of actual damages or \$2500 for each violation, or both. The court may award costs  
220 and reasonable attorneys' fees to a prevailing party, as well as treble damages when the  
221 defendant has engaged in a pattern of violations. The remedies provided in this section do not  
222 preclude the seeking of remedies, including criminal remedies, under any other applicable  
223 provision of law.

224                   SECTION 7. Amend chapter 266 of the General Laws by inserting after section  
225 37F the following section:- Section 37G. (a) For the purposes of this section, the following terms  
226 shall have the following meanings:- "Identity theft" or "Identity fraud", whoever, with intent to  
227 defraud, obtains personal identifying information about another person, or poses as another  
228 person, without the express authorization of that person and uses such person's personal  
229 identifying information to obtain or to attempt to obtain money, credit, goods, services, anything  
230 of value, any identification card or other evidence of such person's identity, or to harass another.  
231 "Identity theft report", a report filed with a law enforcement agency containing specific details of  
232 an identity theft. "Law enforcement agency", any police department of the commonwealth, or  
233 any of its political subdivisions. "Technology based identity theft", deceptively obtaining another  
234 individual's personally identifying information, through use of the Internet, an electronic  
235 database, or any other means of technology. (b) The attorney general, in collaboration with any  
236 law enforcement agency, shall create a uniform identity theft intake procedure for law  
237 enforcement, to include the following: (1) an identity theft report form as required under  
238 subsection (e) of section 37E of chapter 266 that meets the requirements of the Federal Trade  
239 Commission Division of Privacy and Identity Protection Report Form. (2) identify or establish  
240 organizations dedicated to collecting and maintaining information regarding identity theft,  
241 identity fraud and technology based identity theft and identity fraud. (3) transmitting said identity

242 theft report under paragraph (1) to the organizations identified under (b)(2). (4) the creation, in  
243 collaboration with the Federal Trade Commission, and U.S. Secret Service, of a uniform identity  
244 theft resource and instructional steps guide to be presented to all alleged victims. (c) Law  
245 enforcement agencies shall: (1) adhere to the procedure established in subsection (b) when an  
246 identity theft victim files a complaint. (2) participate in any organization deemed appropriate by  
247 the attorney general for combating identity theft. (3) report all identity theft activity to the  
248 Massachusetts Identity Theft and Financial Crimes Task Force, the FTC Clearinghouse  
249 Consumer Sentinel, or any other organizations identified or established by the attorney general  
250 under (b)(2) of this section. (4) report all technology based identity theft activity to the New  
251 England Electronic Crimes Task Force and the Internet Crime Complaint Center. (5) meet  
252 regularly with major banking, financial services and credit institutions, and their leadership, to  
253 discuss cooperative methods to combat identity thieves and assist victims. (6) participate in the  
254 Office of the attorney general’s Cyber Crime Initiative training events pertaining to identity  
255 fraud or identity theft. (7) make available to officers of law enforcement agencies the “Identity  
256 Crime: An Interactive Resource Guide,” a training guide for law enforcement officers published  
257 by a cooperative effort with the U.S. Secret Service, U.S. Postal Inspection Service, Federal  
258 Trade Commission, and the International Association of Chiefs of Police.

259                   SECTION 8. Subsection (a) of section 38 of chapter 22C of the General Laws  
260 is hereby amended by inserting after the word “agencies” in line 4, the following words:-  
261 “information concerning illegal activities generally described as identity theft or identity fraud,”.

262                   SECTION 9. Subsection (d) of section 38 of chapter 22C of the General Laws  
263 is hereby amended by inserting after the word “literature” in line 38, the following words:- “,  
264 identity theft, identity fraud”.

265 SECTION 10. Chapter 6 of the General Laws is hereby amended by inserting  
266 after section 116E the following section:- Section 116F. (a) The municipal police training  
267 committee shall provide instruction for police officers in identifying, responding to and reporting  
268 all incidents of identity fraud, as defined in section 37E of chapter 266. The municipal police  
269 training committee shall include such instruction in all curricula for recruits and in-service  
270 trainees and in all police academies operated or certified by said committee.

271 SECTION 11. Section 2 of chapter 93H of the General Laws is hereby  
272 amended by inserting after subsection (c) the following subsection:- (d) Each state department  
273 and state agency shall enact and maintain a permanent privacy policy that includes, but is not  
274 limited to, the following principles: (1) personal information is only obtained through lawful  
275 means. (2) the purposes for which personal information is collected are specified at or prior to  
276 the time of collection, and any subsequent use is limited to the fulfillment of purposes not  
277 inconsistent with those purposes previously specified. (3) personal information shall not be  
278 disclosed, made available, or otherwise used for purposes other than those specified, except with  
279 the consent of the subject of the data, or as authorized by law or regulation. (4) personal  
280 information collected must be relevant to the purpose for which it is collected. (5) the general  
281 means by which personal information is protected against loss, unauthorized access, use  
282 modification or disclosure shall be posted, unless such disclosure of general means would  
283 compromise legitimate state department or state agency objectives or law enforcement purposes.  
284 (6) each state department or state agency shall designate an individual within that department or  
285 agency to implement the privacy policy within that department or agency.

286 SECTION 12. Chapter 93H of the General Laws is hereby amended by  
287 inserting after section 2 the following new sections:- Section 2A. (a) As used in sections 2A to

288 2B, inclusive, the following words shall have the following meanings, unless the context requires  
289 otherwise:- “Deceptive identification document”, any document not issued by a government  
290 agency of this state, another state, the federal government, a foreign government, a political  
291 subdivision of a foreign government, an international government, or an international quasi-  
292 governmental organization, which purports to be, or which might deceive an ordinary reasonable  
293 person into believing that it is, a document issued by such an agency, including, but not limited  
294 to, a driver’s license, identification card, birth certificate, baptism certificate, passport, or social  
295 security card. “Document-making device”, an implement, tool, equipment, impression, laminate,  
296 card, template, computer file, computer disk, electronic device, hologram, laminate machine or  
297 computer hardware or software. “Password” or “personal identification number”, a unique and  
298 random number or a unique and random combination of numbers, letters or symbols. “Person”,  
299 natural person, corporation, association, state or local agency or political subdivision, partnership  
300 or other legal entity. “Social security number”, the nine digit number assigned by the federal  
301 government as a method to account for an individual’s taxable earnings. (b) No person shall: (1)  
302 intentionally communicate or make available to the public an individual’s social security  
303 number; (2) print a social security number on any card required for the individual to access  
304 products or services provided by the person or entity; (3) require an individual to transmit her  
305 social security number over the Internet, unless the connection is secure or the social security  
306 number is encrypted; (4) require an individual to use her social security number to access an  
307 Internet website, unless a password or personal identification number is also required. (5) print a  
308 social security number on any materials that are mailed to the individual, unless state or federal  
309 law requires the social security number to be on the document. Social Security numbers may be  
310 included in applications and forms sent by mail, including documents sent as part of an

311 application or enrollment process, or to establish, amend or terminate an account, contract or  
312 policy, or to confirm the accuracy of the social security number. A social security number that is  
313 permitted to be mailed under this section may not be printed, in whole or in part, on a postcard or  
314 other mailer not requiring an envelope, or visible on the envelope or without the envelope having  
315 been opened. (6) place a social security number in files with unrestricted employee access; (7)  
316 file a document available for public inspection that contains a social security number of any  
317 other person, unless the person is a dependent child or has consented to the filing. (8) print more  
318 than the last four digits of an employee's social security number on employee pay stubs or  
319 itemized statements. (9) encode or embed a social security number on a card or document after  
320 removing the social security number as required by this statute; (10) sell, lease, lend, trade, rent  
321 an individual's Social Security number; (11) otherwise intentionally disclose to a third party  
322 when the party making the disclosure knows or, in the exercise of reasonable diligence, would  
323 have reason to believe that the third party lacks a legitimate purpose for obtaining the  
324 individual's social security number. (c) Any person that collects social security numbers in the  
325 course of business shall create, and publish or display, a privacy protection policy. (d) No person  
326 needing to identify a resident of the Commonwealth may use that individual's social security  
327 number. That person may, however, assign to that individual some distinguishing number or  
328 mark. This number or mark shall not be the individual's social security number, and shall not  
329 contain any sequence of digits from the individual's social security number. (e) This section does  
330 not prevent the collection, use or release of a social security number as required by state or  
331 federal law. This section does not apply to records that are by statute or case law required to be  
332 made available to the public. (f) Any waiver of the provisions of this section is contrary to public  
333 policy, and is void and unenforceable. (g) Violations of any provision of this section shall

334 constitute an unfair and deceptive trade practice under the provisions of chapter 93A. Section 2B.  
335 (a) Every person who manufactures, produces, sells, offers, or transfers to another any deceptive  
336 identification document knowing such document to be false or counterfeit and with the intent to  
337 deceive, is guilty of a misdemeanor, and upon conviction thereof shall be punished by  
338 imprisonment in the county jail not to exceed 1 year. (b) Every person who offers, displays, or  
339 has in his or her possession any deceptive identification document, or any genuine certificate of  
340 birth which describes a person then living or deceased, with intent to represent himself or herself  
341 as another or to conceal his or her true identity, is guilty of a misdemeanor, and upon conviction  
342 thereof shall be punished by imprisonment in the county jail not to exceed 1 year. (c) Any person  
343 who possesses a document-making device with the intent that the device will be used to  
344 manufacture, alter, or authenticate a deceptive identification document is guilty of a  
345 misdemeanor punishable by imprisonment in a county jail not exceeding one year, or by a fine  
346 not exceeding \$1000, or both. (d) The attorney general, or any district attorney, may prosecute  
347 violators.

348                   SECTION 13. Chapter 93 of the General Laws is hereby amended by inserting  
349 after section 49A the following section:- Section 49B. (a) As used in this section, the following  
350 words shall have the following meanings:- “Debtor”, a natural person who owes money, property  
351 or services to a creditor. “Creditor”, person, organization, company, or government that has  
352 provided some property or service to another party with the understanding that the second party  
353 will repay the debt at a later date, or an attorney or an assignee of such person, or a person or  
354 agency contracted to collect said debt. “Identity theft affidavit”, Federal Trade Commission’s  
355 Affidavit of Identity Theft. “Identity theft passport”, a card or certificate issued by the attorney  
356 general that verifies the identity of the person who is a victim of identity theft or identity fraud.

357 (b) No one who is a creditor of a natural person present or residing in Massachusetts shall engage  
358 in collection activities after receipt from the debtor of the following: (1) a copy of a valid identity  
359 theft report filed by the debtor alleging that the debtor is the victim of an identity theft crime,  
360 including, but not limited to, a violation of section 37E of chapter 266, for the specific debt being  
361 collected by the creditor; and (2) the debtor's written statement that the debtor claims to be the  
362 victim of identity theft with respect to the specific debt being collected by the creditor. This  
363 written statement shall consist of either of the following: (i) a signed Identity Theft affidavit; (ii)  
364 an identity theft passport, as described under subsection (k) or section 37E of chapter 266; or (iii)  
365 a written statement that certifies that the representations are true, correct, and contain no material  
366 omissions of fact to the best knowledge and belief of the person submitting the certification. A  
367 person submitting such certification who declares as true any material matter under this  
368 paragraph that he or she knows to be false is guilty of a misdemeanor. This statement shall  
369 contain, or be accompanied by, any of the following, to the extent that such items are relevant to  
370 the debtor's allegation of identity theft with respect to the debt in question: (A) a statement that  
371 the debtor is a victim of identity theft; (B) a copy of the debtor's driver's license or identification  
372 card, as issued by the state; (C) any other identification document that supports the statement of  
373 identity theft; (D) specific facts supporting the claim of identity theft, if available; (E) any  
374 explanation showing that the debtor did not incur the debt; (F) any available correspondence  
375 disputing the debt after transaction information has been provided to the debtor; (G)  
376 documentation of the residence of the debtor at the time of the alleged debt. This may include  
377 copies of bills and statements, such as utility bills, tax statements, or other statements from  
378 businesses sent to the debtor, showing that the debtor lived at another residence at the time the  
379 debt was incurred; (H) a telephone number for contacting the debtor concerning any additional

380 information or questions, or direction that further communications to the debtor be in writing  
381 only, with the mailing address specified in the statement; (I) the identification of any person  
382 whom the debtor believes is responsible for incurring the debt; (J) an express statement that the  
383 debtor did not authorize the use of the debtor's name or personal information for incurring the  
384 debt. (c) The creditor receiving the materials listed in subparagraph (iii) of paragraph (2) of  
385 subsection (e) shall not release the materials to the public or any other entity. (d) The  
386 certification required under subparagraph (iii) of paragraph (2) of subsection (e) shall be  
387 sufficient if it is in substantially the following form: "I certify the representations made are true,  
388 correct, and contain no material omissions of fact. \_\_\_\_\_."  
389 (Date and Place) (Signature) (e) If a debtor notifies a creditor orally that he or she is a victim of  
390 identity theft, the creditor shall notify the debtor, orally or in writing, that the debtor's claim must  
391 be in writing If a debtor notifies a creditor in writing that he or she is a victim of identity theft,  
392 but omits information required under subsection (e) or, if applicable, the certification required  
393 under subparagraph (iii) of paragraph (2) of subsection (e), and the creditor does not cease  
394 collection activities, the creditor shall provide written notice to the debtor of the additional  
395 information, or the certification required under subparagraph (iii) of paragraph (2) of subsection  
396 (e), that is required, and send the debtor a copy of the Federal Trade Commission's Affidavit of  
397 Identity Theft form. (f) Upon receipt of the complete statement and information described in  
398 subsection (e) of this section, the creditor shall review and consider all of the information  
399 provided by the debtor and other information relevant to the review. The creditor may  
400 recommence debt collection activities only upon making a good faith determination, based on all  
401 of the information provided by the debtor and other information available to the creditor in its  
402 file or from the debtor, that the information does not establish that the debtor is not responsible

403 for the specific debt in question. The creditor's determination shall be made in a manner  
404 consistent with the provisions of 15 U.S.C.1692f(1). The creditor shall notify the debtor in  
405 writing of that determination and the basis for that determination before proceeding with any  
406 further collection activities. (g) No inference or presumption that the debt is valid or invalid, or  
407 that the debtor is liable or not liable for the debt, shall arise if the creditor decides after the  
408 review described in subsection (h) of this section to cease or recommence the debt collection  
409 activities. The exercise or non-exercise of rights under this section is not a waiver of any other  
410 right or defense of the debtor or creditor or debt collector. (h) A creditor who ceases collection  
411 activities under this section and does not recommence those collection activities, shall within 5  
412 business days of the cessation of collection activities, do the following: (1) if the creditor has  
413 furnished adverse information to a consumer credit reporting agency, notify the agency to delete  
414 that information; and (2) notify the creditor that debt collection activities have been terminated  
415 based upon the debtor's claim of identity theft. (i) Failure to comply with the provisions of this  
416 section shall constitute an unfair or deceptive act or practice under the provisions of chapter 93A.

417                   SECTION 14. Section 50 of chapter 93 of the General Laws is hereby amended  
418 by inserting after the definition "Firm offer of credit" the following definition:- "Identity theft  
419 passport", a card or certificate issued by the attorney general that verifies the identity of the  
420 person who is a victim of identity theft or identity fraud. SECTION 15. Section 59 of chapter 93  
421 of the General Laws is hereby amended by adding the following subsections:- (f) Every  
422 consumer credit reporting agency shall, upon the receipt of an identity theft passport, or identity  
423 theft report, from a victim of identity theft, provide the victim, free of charge and upon request,  
424 with up to 12 copies of the victim's consumer report during a consecutive 12-month period  
425 following the date of the police report, not to exceed 1 copy per month. Notwithstanding any

426 other provision of this title, the maximum number of free reports a victim of identity theft is  
427 entitled to obtain under this title is 12 per year. (g) The office of consumer affairs and business  
428 regulations shall adopt regulations to carry out the provisions of this section. The regulations  
429 must include a procedure by which the consumer reporting agency is reasonably assured that the  
430 identity theft victim has an identity fraud claim that is legitimate and adequately substantiated.

431           SECTION 16. Section 62 of chapter 93 of the General Laws is hereby amended  
432 by adding after subsection (c) the following subsections:- (d) No entity that extends credit may  
433 deny credit, reduce the credit limit, or raise the cost of credit of a consumer, solely because such  
434 consumer is a victim of identity theft, if the person denying, reducing, or raising the cost of, the  
435 credit has prior knowledge that the consumer was a victim of identity theft. (e) Actions taken by  
436 a creditor to assist a consumer regarding his or her credit report, credit score or credit history or  
437 to limit credit or financial losses to the consumer, including the cancellation, monitoring or  
438 restructuring of consumer credit accounts, shall not be considered violations of this section. (f)  
439 For purposes of this section, a person is the victim of identity theft, as described under section  
440 37E of chapter 266, if he or she possesses a valid identity theft passport, or identity theft report  
441 alleging that he or she is the victim of an identity theft crime, including, but not limited to, a  
442 violation of section 37E of chapter 266.

443           SECTION 17. The General Laws are hereby amended by inserting after chapter  
444 258E the following chapter:- CHAPTER 258F. RELIEF FOR IDENTITY THEFT VICTIMS  
445 Section 1. As used in this chapter the following words shall have the following meanings:-  
446 “Direct victim” or “Victim of identity theft”, any person or entity whose identity has been  
447 transferred, used, or possessed in violation of section 37E of chapter 266. “Identity theft”  
448 “identity fraud”, whoever, with intent to defraud, obtains personal identifying information about

449 another person, or poses as another person, without the express authorization of that person and  
450 uses such person's personal identifying information to obtain or to attempt to obtain money,  
451 credit, goods, services, anything of value, any identification card or other evidence of such  
452 person's identity, or to harass another. "Identity theft affidavit", Federal Trade Commission's  
453 Affidavit of Identity Theft. "Identity theft report", a report that alleges a violation of section 37E  
454 of chapter 266 of the general laws, 18 United Commonwealths Code, section 1028, or a similar  
455 statute in any other jurisdiction, or a copy of a report filed by a consumer with an appropriate  
456 federal, state or local law enforcement agency, and the filing of which subjects the person filing  
457 the report to criminal penalties pursuant to section 67B of chapter 266 or section 13A of chapter  
458 269. "Person", natural person. Section 2. (a) A person who reasonably believes that he or she is  
459 the victim of identity theft, and that another individual has provided law enforcement or the  
460 judicial system with the person's name after being arrested or indicted for committing a crime,  
461 may receive copies of the following, if applicable: (1) the arrest warrant; (2) the complaint (3)  
462 the indictment; and (4) the judgment of conviction. (b) A person who reasonably believes that he  
463 or she is the victim of identity theft may petition a court, or the court, on its own motion or upon  
464 application of the prosecuting attorney, may move, for an expedited judicial determination of the  
465 person's factual innocence, where the perpetrator of the identity theft was arrested for, cited for,  
466 or convicted of a crime under the victim's identity, or where a criminal complaint has been filed  
467 against the perpetrator in the victim's name, or where the victim's identity has been mistakenly  
468 associated with a record of criminal conviction. (1) The petitioner shall state: (i) the petitioner's  
469 full name; (ii) the petitioner's date of birth; (iii) the petitioner's address; (iv) the specific criminal  
470 charge to be expunged; (v) the date of the arrest; (vi) the name of the arresting agency (vii) the  
471 date of final disposition of the charge as set forth in the petition; and (viii) the full name used by

472 the thief at the time of arrest. (2) The petitioner shall submit the following, if reasonably  
473 available: (i) the identity theft report; (ii) the identity theft passport; (iii) the identity theft  
474 affidavit; (iv) a copy of the complaint; (v) a copy of the warrant; (vi) a copy of the indictment;  
475 (vii) the judgment of conviction; and (viii) any other information ordered to be part of the record  
476 by the court. (3) Where this information is not reasonably available, the petition shall state the  
477 reason for such unavailability. (4) Where the court determines that the petition or motion is  
478 meritorious and that there is no reasonable cause to believe that the victim committed the offense  
479 for which the perpetrator of the identity theft was arrested, cited, convicted, or subject to a  
480 criminal complaint in the victim's name, or that the victim's identity has been mistakenly  
481 associated with a record of criminal conviction, the court shall find the victim factually innocent  
482 of that offense. (5) If the victim is found factually innocent, the court shall issue an order  
483 certifying this determination. This order shall require expungement of the police and court  
484 records relating to the charge, and shall contain a statement that the dismissal and expungement  
485 are ordered pursuant to this subsection. (6) Upon the entry of an order for expungement, the clerk  
486 of the court shall cause a copy of such order to be forwarded to the department of state police  
487 criminal information section. The department of state police shall direct the manner by which the  
488 appropriate expungement or removal of police records shall be effected. (c) The attorney general  
489 shall provide access to identity theft information to: (1) law enforcement agencies; and (2)  
490 individuals who have submitted a petition for court order under chapter 258F.