

SENATE No. 904

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>Second Middlesex and Norfolk</i>
<i>Jason M. Lewis</i>	<i>Fifth Middlesex</i>
<i>Michael F. Rush</i>	<i>Norfolk and Suffolk</i>
<i>Michael O. Moore</i>	<i>Second Worcester</i>
<i>Louis L. Kafka</i>	<i>8th Norfolk</i>
<i>Barbara L'Italien</i>	<i>Second Essex and Middlesex</i>
<i>James B. Eldridge</i>	<i>Middlesex and Worcester</i>
<i>Brian M. Ashe</i>	<i>2nd Hampden</i>
<i>Leonard Mirra</i>	<i>2nd Essex</i>
<i>Steven S. Howitt</i>	<i>4th Bristol</i>
<i>Ruth B. Balsler</i>	<i>12th Middlesex</i>
<i>Carolyn C. Dykema</i>	<i>8th Middlesex</i>
<i>Cynthia S. Creem</i>	<i>First Middlesex and Norfolk</i>
<i>Sal N. DiDomenico</i>	<i>Middlesex and Suffolk</i>
<i>Eric P. Lesser</i>	<i>First Hampden and Hampshire</i>
<i>Robert L. Hedlund</i>	<i>Plymouth and Norfolk</i>
<i>Donald F. Humason, Jr.</i>	<i>Second Hampden and Hampshire</i>
<i>Kate Hogan</i>	<i>3rd Middlesex</i>

<i>Brian A. Joyce</i>	<i>Norfolk, Bristol and Plymouth</i>
<i>Patricia D. Jehlen</i>	<i>Second Middlesex</i>
<i>Anne M. Gobi</i>	<i>Worcester, Hampden, Hampshire and Middlesex</i>
<i>Kathleen O'Connor Ives</i>	<i>First Essex</i>
<i>Timothy J. Toomey, Jr.</i>	<i>26th Middlesex</i>
<i>Marc R. Pacheco</i>	<i>First Plymouth and Bristol</i>
<i>Joan B. Lovely</i>	<i>Second Essex</i>

SENATE No. 904

By Ms. Spilka, a petition (accompanied by bill, Senate, No. 904) of Karen E. Spilka, Jason M. Lewis, Michael F. Rush, Michael O. Moore and other members of the General Court for legislation to protect the Commonwealth's residents from identity theft. The Judiciary.

[SIMILAR MATTER FILED IN PREVIOUS SESSION
SEE SENATE, NO. 793 OF 2013-2014.]

The Commonwealth of Massachusetts

—————
**In the One Hundred and Eighty-Ninth General Court
(2015-2016)**
—————

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 the 2012
2 Official Edition, is hereby amended by inserting before the definition “Harass” the following
3 definition:-

4 “Direct victim”, any person or entity whose identity has been transferred, used, or
5 possessed in violation of this section.

6 SECTION 2. Section 37E of chapter 266 of the General Laws, is hereby amended by
7 inserting after the definition “Harass” the following definitions:-

8 “Identity theft passport”, a card or certificate issued by the attorney general that verifies
9 the identity of the person who is a victim of identity theft or identity fraud.

10 “Identity theft report”, a police incident report filed with a law enforcement agency
11 containing specific details of an identity theft.

12 “Indirect victim”, a corporation that incurs loss or harm as a result of a crime, a
13 government entity that incurs loss or harm as a result of a crime, family members, guardians,
14 custodians of a minor, incompetent, incapacitated, or deceased persons that incurs loss or harm
15 as a result of a crime, but not the person charged with or alleged to have committed the crime.

16 “Law enforcement agency”, any law enforcement organizations of the Commonwealth,
17 or any of its political subdivisions.

18 SECTION 3. Subsection (d) of section 37E of chapter 266 of the General Laws is hereby
19 amended by inserting after the word “fees.” the following clause:-

20 Upon written request by the victim, or by the prosecutor, the court shall provide to the
21 victim, without cost:

22 (1) a certified copy of the complaint filed in the matter;

23 (2) the judgment of conviction; and

24 (3) an order setting forth the facts and circumstances of the offense.

25 SECTION 4. Section 37E of chapter 266 of the General Laws is hereby amended by
26 striking out subsection (e) and inserting in place thereof the following subsection:-

27 (e) A person who has learned, or reasonably suspects that the person’s personal
28 identifying information has been unlawfully obtained or used by another, may initiate a law
29 enforcement investigation by contacting the local law enforcement that has jurisdiction over the

30 person's residence. A law enforcement officer shall accept an identity theft report from such
31 victim and shall provide a copy to such victim, within 24 hours. Such police incident reports may
32 be filed in any county where a victim resides or has a place of business, or in any county where
33 the breach of security occurred, in whole or in part. The local law enforcement agency with
34 whom the victim filed the initial complaint under this section shall begin an investigation of the
35 facts, and shall, if the suspect resides in another jurisdiction, or if the suspected crime was
36 committed in a different jurisdiction, or if information pertaining to the crime exists in another
37 jurisdiction, notify the law enforcement agency in that jurisdiction of the matter.

38 SECTION 5. Section 37E of chapter 266 of the General Laws is hereby amended by
39 inserting after subsection (f) the following subsections:-

40 (g) (1) The department of state police may initiate investigations and enforce this section
41 throughout the Commonwealth without regard to any limitation otherwise applicable to the
42 department's activities in a municipality or other political subdivision. The authority granted in
43 this subsection may be exercised only in accordance with regulations that the department of state
44 police adopts.

45 (2) A law enforcement officer of a municipality or county may investigate violations of
46 this section throughout the Commonwealth without any limitation as to jurisdiction and to the
47 same extent as a law enforcement officer of the department of state police. The authority granted
48 in this subsection may be exercised only if an act related to the crime was committed in the
49 investigating law enforcement agency's jurisdiction or if the complaining witness resides, or has
50 a principal place of business, in the investigating law enforcement agency's jurisdiction.

51 (3) A law enforcement officer may arrest, without a warrant, any person he has probable
52 cause to believe has committed the offense of identity fraud as defined in this section.

53 (h) If a state, municipal or county law enforcement agency takes action under the
54 authority granted in subsection (g) of this section, the law enforcement agency granted authority
55 under said subsection (g) shall collaborate with the law enforcement agency to be notified of an
56 investigation. Notification of an investigation:

57 (1) in a municipal corporation, shall be made to the chief of police or designee of the
58 chief of police;

59 (2) in Boston, shall be made to the Police Commissioner or the Police Commissioner's
60 designee; and

61 (3) on property owned, leased, or operated by or under the control of the Massachusetts
62 Bay Transportation Authority or the Massachusetts Port Authority, shall be made to the
63 respective chief of police or the chief's designee.

64 (i) (1) A district attorney or the attorney general may investigate and prosecute a
65 violation of this section or a violation of any crime based on the act establishing a violation of
66 this section.

67 (j) In any criminal proceeding brought under this section, the crime is considered to be
68 committed in the municipality:

69 (1) where the direct victim, or indirect victim resides or has a place of business;

70 (3) where any part of the violation occurred, regardless of whether the defendant was
71 ever actually present in that municipality; or

72 (4) in any other municipality instrumental to the completion of the offense, regardless of
73 whether the defendant was ever physically present in that municipality.

74 (k) In addition to the criminal penalties in subsections (d), of this section, any person who
75 commits an act made unlawful by this section shall be liable to the person to whom the
76 identifying information belonged, or the entity that suffered financial loss, for civil damages.

77 (1) A victim under this section may bring an action in the superior court of her county of
78 residence, or any county in which any part of the act took place, regardless of whether the person
79 who committed the violation was ever physically present in that municipality.

80 (2) The victim may institute a civil action to:

81 (i) Enjoin and restrain future acts that would constitute a violation of this section;

82 (ii) Recover \$5000 for each incident, or 3 times actual damages, whichever is greater;

83 (iii) Recover reasonable attorneys' fees and costs; and

84 (iv) Additional relief the court deems necessary.

85 (3) A financial institution, insurance company, or business that suffers direct financial
86 loss as a result of the offense may bring an action under this section and shall also be entitled to
87 damages, but damages to natural persons shall be fully satisfied prior to any payment to a
88 financial institution, insurance company, bonding association or business.

89 (4) If the identifying information of a deceased person is used in a manner made unlawful
90 by this section, or any other general or special law, the deceased person's estate shall have the
91 right to recover damages.

92 (5) No action under this section shall be brought but within five years from the date when
93 the violation is discovered or, in the exercise of reasonable care, should have been discovered.

94 (6) Civil action under this section does not depend on whether or not a criminal
95 prosecution has been, or will be, instituted under this section for the acts which are the subject of
96 the civil action.

97 (7) A final judgment rendered in favor of the Commonwealth in any criminal proceeding
98 shall estop the defendant from denying the same conduct in any civil action brought pursuant to
99 this section.

100 (1) (1) A natural person who has, under this section, filed, with a law enforcement agency,
101 a police report alleging identity theft under this section, may apply for an identity theft passport
102 through any law enforcement agency, or directly through the attorney general. A law
103 enforcement agency that receives an application for an identity theft passport shall submit the
104 application and a copy of the identity theft report to the attorney general for processing and
105 issuance of an identity theft passport. The attorney general, in cooperation with any law
106 enforcement agency in the Commonwealth, may issue an identity theft passport to a person who
107 is a victim of identity theft in this Commonwealth and who has filed a police report citing that
108 such person is a victim of a violation of this chapter. This passport shall be in the form of a card
109 or certificate, and must include photo identification.

110 (2) The attorney general shall perform a background check on the identity theft victim
111 before issuing an identity theft passport under this section.

112 (3) An identity theft victim who has been issued an identity theft passport under this
113 section may present this identity theft passport to:

114 (i) a law enforcement agency to help prevent the arrest or detention of the person for an
115 offense committed by another using the person's personal identifying information; or

116 (ii) any of the victim's creditors to aid in the investigation of:

117 (A) a fraudulent account that was opened in the person's name; or

118 (B) a fraudulent charge that is made against an account of the person.

119 (iii) A consumer reporting agency, as defined in § 603(f) of the federal Fair Credit
120 Reporting Act (15 U.S.C. § 1681a(f)), to expedite removal of accounts opened fraudulently by
121 another and correcting credit report information.

122 (4) A law enforcement agency or creditor that is presented with an identity theft passport
123 under subsections (3)(i) or (3)(ii) of this section has sole discretion to accept or reject the identity
124 theft passport. The consumer reporting agency must accept the passport as an official notice of a
125 dispute and must include notice of the dispute in all future reports that contain disputed
126 information caused by the identity fraud.

127 (5) An application for an identity theft passport submitted under this section, including
128 any supporting documentation:

129 (i) is not a public record; and

130 (ii) may not be released except to a law enforcement agency in any state.

131 (6) The attorney general shall adopt regulations to carry out the provisions of this section.

132 The regulations must include a procedure by which the Office of the attorney general is

133 reasonably assured that an identity theft passport applicant has an identity fraud claim that is
134 legitimate and adequately substantiated.

135 SECTION 6. Chapter 266 of the General Laws is hereby amended by inserting after
136 section 37E the following section:-

137 Section 37F. (a) For purpose of this section, the following words and terms shall have
138 the following meanings:-

139 "Advertisement", means a communication, the primary purpose of which is the
140 commercial promotion of a commercial product or service, including content on an Internet Web
141 site operated for a commercial purpose.

142 "Authorized user", with respect to a computer, means a person who owns or is authorized
143 by the owner or lessee to use the computer. An "authorized user" does not include a person or
144 entity that has obtained authorization to use the computer solely through the use of an end user
145 license agreement.

146 "Computer or Internet settings", security or other settings that protect information about
147 the authorized user, any page that appears when an authorized user launches an Internet browser
148 or similar software program used to access and navigate the Internet, the default provider or Web
149 proxy the authorized user uses to access or search the Internet, the authorized user's list of
150 bookmarks used to access Web pages.

151 "Computer software", a sequence of instructions written in any programming language
152 that is executed on a computer.

153 “Computer virus” means a computer program or other set of instructions that is designed
154 to degrade the performance of or disable a computer or computer network and is designed to
155 have the ability to replicate itself on other computers or computer networks without the
156 authorization of the owners of those computers or computer networks.

157 “Consumer” means an individual who resides in this state and who uses the computer in
158 question primarily for personal, family, or household purposes.

159 “Damage” means any significant impairment to the integrity or availability of data,
160 software, a system, or information.

161 “Execute,” when used with respect to computer software, means the performance of the
162 functions or the carrying out of the instructions of the computer software.

163 “Intentionally deceptive,” by means of an intentionally and materially false or fraudulent
164 statement, by means of a statement or description that intentionally omits or misrepresents
165 material information in order to deceive the consumer, by means of an intentional and material
166 failure to provide any notice to an authorized user regarding the download or installation of
167 software in order to deceive the consumer.

168 “Internet” means the global information system that is logically linked together by a
169 globally unique address space based on the Internet Protocol (IP), or its subsequent extensions,
170 and that is able to support communications using the Transmission Control Protocol/Internet
171 Protocol (TCP/IP) suite, or its subsequent extensions, or other IP-compatible protocols, and that
172 provides, uses, or makes accessible, either publicly or privately, high level services layered on
173 the communications and related infrastructure described in this subdivision.

174 “Payment card”, a credit card, debit card, or any other card that is issued to an authorized
175 user and that allows the user to obtain, purchase, or receive goods, services, money, or
176 anything else of value.

177 “Person”, any natural person, business, or state or local agency or political subdivision.

178 “Personally identifiable information”, any name or number that may be used, alone or in
179 conjunction with any other information, to assume the identity of an individual, including any
180 name, address, telephone number, driver’s license number, social security number, place of
181 employment, employee identification number, mother’s maiden name, demand deposit account
182 number, savings account number, credit card number or computer password identification.

183 “Reencoder”, an electronic device that places encoded information from the magnetic
184 strip or stripe of a payment card on to the magnetic strip or stripe of a payment card on to the
185 magnetic strip or stripe of a different payment card.

186 “Scanning device”, a scanner, reader, or any other electronic device that is used to access,
187 read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the
188 magnetic strip or stripe of a payment card.

189 “Skimming device”, a machine or instrument used to deceptively access, read, scan,
190 obtain, memorize, or store, temporarily or permanently, payment card information or a person’s
191 personal identification number, used in an otherwise legitimate transaction.

192 (b) Any person who is not an authorized user shall not:

193 (1) Transmit computer software to the authorized user's computer with actual
194 knowledge, or with conscious avoidance of actual knowledge, and to use such software, through
195 intentionally deceptive means, to:

196 (i) collect personally identifiable information, or collect information that meets any of the
197 following criteria:

198 (A) All keystrokes made by an authorized user who uses the computer and transfer that
199 information from the computer to another person;

200 (B) The Internet sites visited by an authorized user.

201 (ii) modify computer or Internet settings;

202 (iii) prevent an authorized user's reasonable efforts to block installation, or execution of,
203 or to disable, software, by:

204 (A) falsely representing that software has been disabled.

205 (B) causing software that the authorized user has properly removed or disabled to
206 automatically reinstall or reactivate on the computer without the authorization of an authorized
207 user;

208 (C) presenting the authorized user with an option to decline installation of software with
209 knowledge that, when the option is selected by the authorized user, the installation nevertheless
210 proceeds.

211 (iv) remove, disable, or render inoperative security, antispyware or antivirus computer
212 software;

213 (v) take control, through intentionally deceptive means, of the consumer's computer;

214 (vi) deceptively install, and execute, on the computer one or more additional computer
215 software components with the intent of causing an authorized user to use the components in a
216 way that violates any other provision of this section;

217 (vii) access or use the consumer's modem or Internet service for the purpose of causing
218 damage to the consumer's computer or causing an authorized user to incur unauthorized financial
219 charges;

220 (viii) use the consumer's computer as part of an activity performed by a group of
221 computers for the purpose of causing damage to another computer, including launching a denial
222 of service attack;

223 (ix) open multiple, sequential, stand-alone advertisements in the consumer's Internet
224 browser, without the authorization of an authorized user, and with knowledge that a reasonable
225 computer user cannot close the advertisements without turning off the computer or closing the
226 consumer's Internet browser;

227 (2) Through any means, technology based or not technology based, including but not
228 limited to the use of an Internet site, electronic mail message, or otherwise through use of the
229 Internet, or through the use of a telephone call, fax machine, in-person interaction or other type
230 of interaction, to solicit, request, or take action to induce another person to provide identifying
231 information by representing itself to be a person, business or organization without the authority
232 or approval of such person, business or organization.

233 (c) No person shall knowingly, willfully, and with the intent to defraud, possess or use:

234 (1) a scanning device to access, read, obtain, memorize or store, temporarily or
235 permanently, information encoded on the magnetic strip or stripe of a payment card without the
236 permission of the authorized user of the payment card;

237 (2) a reencoder to place encoded information on the magnetic strip or stripe of a payment
238 card or any electronic medium that allows an authorized transaction to occur, without the
239 permission of the authorized user of the payment card from which the information is being
240 reencoded;

241 (3) a skimming device, or a camera, to obtain the account number or PIN of a payment
242 card or any electronic medium that allows an authorized transaction to occur, without the
243 permission of the authorized user of the payment card from which the information is being
244 skimmed.

245 (d) Any scanning device or reencoder or skimming device described in this section
246 owned by the defendant and possessed or used in violation of subsection (c) may be seized and
247 be destroyed as contraband by law enforcement officials of the jurisdiction in which the scanning
248 device or reencoder or skimming device was seized.

249 (e) Any computer, computer system, computer network, or any software or data, owned
250 by the defendant, which is used during the commission of any public offense described in this
251 section, or any computer, owned by the defendant, which is used as a repository for the storage
252 of software or data illegally obtained in violation of this section shall be subject to forfeiture.

253 (f) Nothing in this section shall apply to any monitoring of, or interaction with, a
254 subscriber's Internet or other network connection or service, or a protected computer, by a
255 telecommunications carrier, cable operator, computer hardware or software provider, or provider

256 of information service or interactive computer service for network or computer security
257 purposes, diagnostics, technical support, repair, authorized updates of software or system
258 firmware, authorized remote system management, or detection or prevention of the unauthorized
259 use of or fraudulent or other illegal activities in connection with a network, service, or computer
260 software, including scanning for and removing software proscribed under this chapter.

261 (g) Any person who violates this section shall be guilty of a misdemeanor, punishable by
262 a term in a county jail or house of correction not to exceed 1 year, or a fine of \$1,000, or both the
263 imprisonment and fine.

264 (h) Any person who violates this section and sells, distributes, or uses such information
265 shall be guilty of a felony and punished by a fine of not more than \$5,000 or imprisonment in a
266 state prison for not more than 2 1/2 years, or by both such fine and imprisonment.

267 (i) The attorney general may bring an action against a person who committed a violation
268 under this section to enjoin further violations, recover a civil penalty of up to \$2500 per
269 violation, or both.

270 SECTION 7. Amend chapter 266 of the General Laws by inserting after section 37F the
271 following section:-

272 Section 37G. (a) For the purposes of this section, the following terms shall have the
273 following meanings:-

274 “Identity theft” or “Identity fraud”, whoever, with intent to defraud, obtains personal
275 identifying information about another person, or poses as another person, without the express
276 authorization of that person and uses such person’s personal identifying information to obtain or

277 to attempt to obtain money, credit, goods, services, anything of value, any identification card or
278 other evidence of such person's identity, or to harass another.

279 "Identity theft report", a report filed with a law enforcement agency containing specific
280 details of an identity theft.

281 "Law enforcement agency", any police department of the commonwealth, or any of its
282 political subdivisions.

283 "Technology based identity theft", deceptively obtaining another individual's personally
284 identifying information, through use of the Internet, an electronic database, or any other means
285 of technology.

286 (b) The attorney general, in collaboration with any law enforcement agency, shall create a
287 uniform identity theft intake procedure for law enforcement, to include the following:

288 (1) an identity theft report form as required under subsection (e) of section 37E of chapter
289 266 that meets the requirements of the Federal Trade Commission Division of Privacy and
290 Identity Protection Report Form.

291 (2) identify or establish organizations dedicated to collecting and maintaining information
292 regarding identity theft, identity fraud and technology based identity theft and identity fraud.

293 (3) transmitting said identity theft report under paragraph (1) to the organizations
294 identified under (b)(2).

295 (c) The attorney general shall create a uniform identity theft resource and instructional
296 steps guide for victims, and maintain a publicly accessible copy of said guide on its website. The
297 attorney general shall review said guide on an annual basis and update it as necessary. A law

298 enforcement agency which receives a report of identity theft or identity fraud in violation of this
299 section shall provide a physical copy of said resource guide to the victim within 24 hours of
300 receiving the report of identity theft or identity fraud.

301 (d) Law enforcement agencies shall:

302 (1) adhere to the procedure established in subsection (b) when an identity theft victim
303 files a complaint.

304 (2) participate in any organization deemed appropriate by the attorney general for
305 combating identity theft.

306 (3) report all identity theft activity to the Massachusetts Identity Theft and Financial
307 Crimes Task Force, the FTC Clearinghouse Consumer Sentinel, or any other organizations
308 identified or established by the attorney general under (b)(2) of this section.

309 (4) report all technology based identity theft activity to the New England Electronic
310 Crimes Task Force and the Internet Crime Complaint Center.

311 (5) meet regularly with major banking, financial services and credit institutions, and their
312 leadership, to discuss cooperative methods to combat identity thieves and assist victims.

313 (6) participate in the Office of the attorney general's Cyber Crime Initiative training
314 events pertaining to identity fraud or identity theft.

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

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

321 SECTION 10. Chapter 6 of the General Laws is hereby amended by inserting after
322 section 116F the following section:-

323 Section 116G. (a) The municipal police training committee shall provide instruction for
324 police officers in identifying, responding to and reporting all incidents of identity fraud, as
325 defined in section 37E of chapter 266. The municipal police training committee shall include
326 such instruction in all curricula for recruits and in-service trainees and in all police academies
327 operated or certified by said committee.

328 SECTION 11. Section 2 of chapter 93H of the General Laws is hereby amended by
329 inserting after subsection (c) the following subsection:-

330 (d) Each state department and state agency shall enact and maintain a permanent privacy
331 policy that includes, but is not limited to, the following principles:

332 (1) personal information is only obtained through lawful means.

333 (2) the purposes for which personal information is collected are specified at or prior to
334 the time of collection, and any subsequent use is limited to the fulfillment of purposes not
335 inconsistent with those purposes previously specified.

336 (3) personal information shall not be disclosed, made available, or otherwise used for
337 purposes other than those specified, except with the consent of the subject of the data, or as
338 authorized by law or regulation.

339 (4) personal information collected must be relevant to the purpose for which it is
340 collected.

341 (5) the general means by which personal information is protected against loss,
342 unauthorized access, use modification or disclosure shall be posted, unless such disclosure of
343 general means would compromise legitimate state department or state agency objectives or law
344 enforcement purposes.

345 (6) each state department or state agency shall designate an individual within that
346 department or agency to implement the privacy policy within that department or agency.

347 SECTION 12. Chapter 93H of the General Laws is hereby amended by inserting after
348 section 2 the following new sections:-

349 Section 2A. (a) As used in sections 2A to 2B, inclusive, the following words shall have
350 the following meanings, unless the context requires otherwise:-

351 “Deceptive identification document”, any document not issued by a government agency
352 of this state, another state, the federal government, a foreign government, a political subdivision
353 of a foreign government, an international government, or an international quasi-governmental
354 organization, which purports to be, or which might deceive an ordinary reasonable person into
355 believing that it is, a document issued by such an agency, including, but not limited to, a driver’s
356 license, identification card, birth certificate, baptism certificate, passport, or social security card.

357 “Document-making device”, an implement, tool, equipment, impression, laminate, card,
358 template, computer file, computer disk, electronic device, hologram, laminate machine or
359 computer hardware or software.

360 “Password” or “personal identification number”, a unique and random number or a
361 unique and random combination of numbers, letters or symbols.

362 “Person”, natural person, corporation, association, state or local agency or political
363 subdivision, partnership or other legal entity.

364 “Social security number”, the nine digit number assigned by the federal government as a
365 method to account for an individual’s taxable earnings.

366 (b) No person shall:

367 (1) intentionally communicate or make available to the public an individual’s social
368 security number;

369 (2) print a social security number on any card required for the individual to access
370 products or services provided by the person or entity;

371 (3) require an individual to transmit her social security number over the Internet, unless
372 the connection is secure or the social security number is encrypted;

373 (4) require an individual to use her social security number to access an Internet website,
374 unless a password or personal identification number is also required.

375 (5) print a social security number on any materials that are mailed to the individual,
376 unless state or federal law requires the social security number to be on the document. Social
377 Security numbers may be included in applications and forms sent by mail, including documents
378 sent as part of an application or enrollment process, or to establish, amend or terminate an
379 account, contract or policy, or to confirm the accuracy of the social security number. A social
380 security number that is permitted to be mailed under this section may not be printed, in whole or

381 in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or
382 without the envelope having been opened.

383 (6) place a social security number in files with unrestricted employee access;

384 (7) file a document available for public inspection that contains a social security number
385 of any other person, unless the person is a dependent child or has consented to the filing.

386 (8) print more than the last four digits of an employee's social security number on
387 employee pay stubs or itemized statements.

388 (9) encode or embed a social security number on a card or document after removing the
389 social security number as required by this statute;

390 (10) sell, lease, lend, trade, rent an individual's Social Security number;

391 (11) otherwise intentionally disclose to a third party when the party making the disclosure
392 knows or, in the exercise of reasonable diligence, would have reason to believe that the third
393 party lacks a legitimate purpose for obtaining the individual's social security number.

394 (c) Any person that collects social security numbers in the course of business shall
395 create, and publish or display, a privacy protection policy.

396 (d) No person needing to identify a resident of the Commonwealth may use that
397 individual's social security number as a primary means of identification. That person may,
398 however, assign to that individual some distinguishing number or mark. This number or mark
399 shall not be the individual's social security number, and shall not contain any sequence of digits
400 from the individual's social security number.

401 (e) This section does not prevent the collection, use or release of a social security
402 number as required by state or federal law. This section does not apply to records that are by
403 statute or case law required to be made available to the public.

404 (f) Any waiver of the provisions of this section is contrary to public policy, and is void
405 and unenforceable.

406 (g) Violations of any provision of this section shall constitute an unfair and deceptive
407 trade practice under the provisions of chapter 93A.

408 Section 2B. (a) Every person who manufactures, produces, sells, offers, or transfers to
409 another any deceptive identification document knowing such document to be false or counterfeit
410 and with the intent to deceive, is guilty of a misdemeanor, and upon conviction thereof shall be
411 punished by imprisonment in the county jail not to exceed 1 year.

412 (b) Every person who offers, displays, or has in his or her possession any deceptive
413 identification document, or any genuine certificate of birth which describes a person then living
414 or deceased, without the authority or approval of such person, with intent to represent himself or
415 herself as such person and with the intent to use such person's identity in a way that is
416 reasonably likely to cause such person substantial physical, emotional, financial or reputational
417 harm, is guilty of a misdemeanor, and upon conviction thereof shall be punished by
418 imprisonment in the county jail not to exceed 1 year.

419 (c) Any person who possesses a document-making device with the intent that the device
420 will be used to manufacture, alter, or authenticate a deceptive identification document is guilty of
421 a misdemeanor punishable by imprisonment in a county jail not exceeding one year, or by a fine
422 not exceeding \$1000, or both.

423 (d) The attorney general, or any district attorney, may prosecute violators.

424 SECTION 13. Section 3 of Chapter 93H of the General Laws is hereby amended by
425 inserting after the words “unreasonable delay,” in line 4, the following words:- “but no later than
426 30 days,”, and by inserting after the words “unreasonable delay,” in line 21, the following
427 words:- “but no later than 30 days,”.

428 SECTION 14. Section 4 of Chapter 93H of the General Laws is hereby amended by
429 striking out the word “delay.” in line 9, and inserting in the place thereof the following words:-
430 “delay, but no later than 7 days after the law enforcement agency informs the person or agency
431 that notification no longer poses a risk of impeding an investigation.”

432 SECTION 15. Chapter 93 of the General Laws is hereby amended by inserting after
433 section 49A the following section:-

434 Section 49B. (a) As used in this section, the following words shall have the following
435 meanings:-

436 “Debtor”, a natural person who owes money, property or services to a creditor.

437 “Creditor”, person, organization, company, or government that has provided some
438 property or service to another party with the understanding that the second party will repay the
439 debt at a later date, or an attorney or an assignee of such person, or a person or agency contracted
440 to collect said debt.

441 “Identity theft affidavit”, Federal Trade Commission’s Affidavit of Identity Theft.

442 “Identity theft passport”, a card or certificate issued by the attorney general that verifies
443 the identity of the person who is a victim of identity theft or identity fraud.

444 (b) No one who is a creditor of a natural person present or residing in Massachusetts shall
445 engage in collection activities after receipt from the debtor of the following:

446 (1) a copy of a valid identity theft report filed by the debtor alleging that the debtor is the
447 victim of an identity theft crime, including, but not limited to, a violation of section 37E of
448 chapter 266, for the specific debt being collected by the creditor; and

449 (2) the debtor's written statement that the debtor claims to be the victim of identity theft
450 with respect to the specific debt being collected by the creditor. This written statement shall
451 consist of either of the following:

452 (i) a signed Identity Theft affidavit;

453 (ii) an identity theft passport, as described under subsection (k) or section 37E of chapter
454 266; or

455 (iii) a written statement that certifies that the representations are true, correct, and contain
456 no material omissions of fact to the best knowledge and belief of the person submitting the
457 certification. A person submitting such certification who declares as true any material matter
458 under this paragraph that he or she knows to be false is guilty of a misdemeanor. This statement
459 shall contain, or be accompanied by, any of the following, to the extent that such items are
460 relevant to the debtor's allegation of identity theft with respect to the debt in question:

461 (A) a statement that the debtor is a victim of identity theft;

462 (B) a copy of the debtor's driver's license or identification card, as issued by the state;

463 (C) any other identification document that supports the statement of identity theft;

464 (D) specific facts supporting the claim of identity theft, if available;

465 (E) any explanation showing that the debtor did not incur the debt;

466 (F) any available correspondence disputing the debt after transaction information has
467 been provided to the debtor;

468 (G) documentation of the residence of the debtor at the time of the alleged debt. This
469 may include copies of bills and statements, such as utility bills, tax statements, or other
470 statements from businesses sent to the debtor, showing that the debtor lived at another residence
471 at the time the debt was incurred;

472 (H) a telephone number for contacting the debtor concerning any additional information
473 or questions, or direction that further communications to the debtor be in writing only, with the
474 mailing address specified in the statement;

475 (I) the identification of any person whom the debtor believes is responsible for incurring
476 the debt;

477 (J) an express statement that the debtor did not authorize the use of the debtor's name or
478 personal information for incurring the debt.

479 (c) The creditor receiving the materials listed in subparagraph (iii) of paragraph (2) of
480 subsection (e) shall not release the materials to the public or any other entity, except as otherwise
481 required by law.

482 (d) The certification required under subparagraph (iii) of paragraph (2) of subsection (e)
483 shall be sufficient if it is in substantially the following form:

484 "I certify the representations made are true, correct, and contain no material omissions of
485 fact. _____."

486 (Date and Place) (Signature)

487 (e) If a debtor notifies a creditor orally that he or she is a victim of identity theft, the
488 creditor shall notify the debtor, orally or in writing, that the debtor's claim must be in writing If a
489 debtor notifies a creditor in writing that he or she is a victim of identity theft, but omits
490 information required under subsection (e) or, if applicable, the certification required under
491 subparagraph (iii) of paragraph (2) of subsection (e), and the creditor does not cease collection
492 activities, the creditor shall provide written notice to the debtor of the additional information, or
493 the certification required under subparagraph (iii) of paragraph (2) of subsection (e), that is
494 required, and send the debtor a copy of the Federal Trade Commission's Affidavit of Identity
495 Theft form.

496 (f) Upon receipt of the complete statement and information described in subsection (e) of
497 this section, the creditor shall review and consider all of the information provided by the debtor
498 and other information relevant to the review. The creditor may recommence debt collection
499 activities only upon making a good faith determination, based on all of the information provided
500 by the debtor and other information available to the creditor in its file or from the debtor, that the
501 information does not establish that the debtor is not responsible for the specific debt in question.
502 The creditor's determination shall be made in a manner consistent with the provisions of 15
503 U.S.C.1692 f(1). The creditor shall notify the debtor in writing of that determination and the
504 basis for that determination before proceeding with any further collection activities.

505 (g) No inference or presumption that the debt is valid or invalid, or that the debtor is
506 liable or not liable for the debt, shall arise if the creditor decides after the review described in
507 subsection (h) of this section to cease or recommence the debt collection activities. The exercise
508 or non-exercise of rights under this section is not a waiver of any other right or defense of the
509 debtor or creditor or debt collector.

510 (h) A creditor who ceases collection activities under this section and does not
511 recommence those collection activities, shall within 5 business days of the cessation of collection
512 activities, do the following:

513 (1) if the creditor has furnished adverse information to a consumer credit reporting
514 agency, notify the agency to delete that information; and

515 (2) notify the creditor that debt collection activities have been terminated based upon the
516 debtor's claim of identity theft.

517 (i) Failure to comply with the provisions of this section shall constitute an unfair or
518 deceptive act or practice under the provisions of chapter 93A.

519 SECTION 16. Section 50 of chapter 93 of the General Laws is hereby amended by
520 inserting after the definition "Firm offer of credit" the following definition:-

521 "Identity theft passport", a card or certificate issued by the attorney general that verifies
522 the identity of the person who is a victim of identity theft or identity fraud.

523 SECTION 17. Section 59 of chapter 93 of the General Laws is hereby amended by
524 adding the following subsections:-

525 (f) Every consumer credit reporting agency shall, upon the receipt of an identity theft
526 passport, or identity theft report, from a victim of identity theft, provide the victim, free of charge
527 and upon request, with up to 12 copies of the victim's consumer report during a consecutive 12-
528 month period following the date of the police report, not to exceed 1 copy per month.
529 Notwithstanding any other provision of this title, the maximum number of free reports a victim
530 of identity theft is entitled to obtain under this title is 12 per year.

531 (g) The office of consumer affairs and business regulations shall adopt regulations to
532 carry out the provisions of this section. The regulations must include a procedure by which the
533 consumer reporting agency is reasonably assured that the identity theft victim has an identity
534 fraud claim that is legitimate and adequately substantiated.

535 SECTION 18. Section 62 of chapter 93 of the General Laws is hereby amended by
536 adding after subsection (c) the following subsections:-

537 (d) No entity that extends credit may deny credit, reduce the credit limit, or raise the cost
538 of credit of a consumer, solely because such consumer is a victim of identity theft, if the person
539 denying, reducing, or raising the cost of, the credit has prior knowledge that the consumer was a
540 victim of identity theft.

541 (e) Actions taken by a creditor to assist a consumer regarding his or her credit report,
542 credit score or credit history or to limit credit or financial losses to the consumer, including the
543 cancellation, monitoring or restructuring of consumer credit accounts, shall not be considered
544 violations of this section.

545 (f) For purposes of this section, a person is the victim of identity theft, as described under
546 section 37E of chapter 266, if he or she possesses a valid identity theft passport, or identity theft

547 report alleging that he or she is the victim of an identity theft crime, including, but not limited to,
548 a violation of section 37E of chapter 266.

549 SECTION 19. The General Laws are hereby amended by inserting after chapter 258E the
550 following chapter:-

551 CHAPTER 258F.

552 RELIEF FOR IDENTITY THEFT VICTIMS

553 Section 1. As used in this chapter the following words shall have the following
554 meanings:-

555 “Direct victim” or “Victim of identity theft”, any person or entity whose identity has been
556 transferred, used, or possessed in violation of section 37E of chapter 266.

557 “Identity theft” “identity fraud”, whoever, with intent to defraud, obtains personal
558 identifying information about another person, or poses as another person, without the express
559 authorization of that person and uses such person’s personal identifying information to obtain or
560 to attempt to obtain money, credit, goods, services, anything of value, any identification card or
561 other evidence of such person’s identity, or to harass another.

562 “Identity theft affidavit”, Federal Trade Commission’s Affidavit of Identity Theft.

563 “Identity theft report”, a report that alleges a violation of section 37E of chapter 266 of
564 the general laws, 18 United Commonwealths Code, section 1028, or a similar statute in any other
565 jurisdiction, or a copy of a report filed by a consumer with an appropriate federal, state or local
566 law enforcement agency, and the filing of which subjects the person filing the report to criminal
567 penalties pursuant to section 67B of chapter 266 or section 13A of chapter 269.

568 “Person”, natural person.

569 Section 2. (a) A person who reasonably believes that he or she is the victim of identity
570 theft, and that another individual has provided law enforcement or the judicial system with the
571 person’s name after being arrested or indicted for committing a crime, may receive copies of the
572 following, if applicable:

573 (1) the arrest warrant;

574 (2) the complaint

575 (3) the indictment; and

576 (4) the judgment of conviction.

577 (b) A person who reasonably believes that he or she is the victim of identity theft may
578 petition a court, or the court, on its own motion or upon application of the prosecuting attorney,
579 may move, for an expedited judicial determination of the person’s factual innocence, where the
580 perpetrator of the identity theft was arrested for, cited for, or convicted of a crime under the
581 victim's identity, or where a criminal complaint has been filed against the perpetrator in the
582 victim's name, or where the victim's identity has been mistakenly associated with a record of
583 criminal conviction.

584 (1) The petitioner shall state:

585 (i) the petitioner’s full name;

586 (ii) the petitioner's date of birth;

587 (iii) the petitioner’s address;

- 588 (iv) the specific criminal charge to be expunged;
- 589 (v) the date of the arrest;
- 590 (vi) the name of the arresting agency
- 591 (vii) the date of final disposition of the charge as set forth in the petition; and
- 592 (viii) the full name used by the thief at the time of arrest.

593 (2) The petitioner shall submit the following, if reasonably available:

- 594 (i) the identity theft report;
- 595 (ii) the identity theft passport;
- 596 (iii) the identity theft affidavit;
- 597 (iv) a copy of the complaint;
- 598 (v) a copy of the warrant;
- 599 (vi) a copy of the indictment;
- 600 (vii) the judgment of conviction; and
- 601 (viii) any other information ordered to be part of the record by the court.

602 (3) Where this information is not reasonably available, the petition shall state the reason
603 for such unavailability.

604 (4) Where the court determines that the petition or motion is meritorious and that there is
605 no reasonable cause to believe that the victim committed the offense for which the perpetrator of

606 the identity theft was arrested, cited, convicted, or subject to a criminal complaint in the victim's
607 name, or that the victim's identity has been mistakenly associated with a record of criminal
608 conviction, the court shall find the victim factually innocent of that offense.

609 (5) If the victim is found factually innocent, the court shall issue an order certifying this
610 determination. This order shall require expungement of the police and court records relating to
611 the charge, and shall contain a statement that the dismissal and expungement are ordered
612 pursuant to this subsection.

613 (6) Upon the entry of an order for expungement, the clerk of the court shall cause a copy
614 of such order to be forwarded to the department of state police criminal information section. The
615 department of state police shall direct the manner by which the appropriate expungement or
616 removal of police records shall be effected.

617 (c) The attorney general shall provide access to identity theft information to: (1) law
618 enforcement agencies; and (2) individuals who have submitted a petition for a court order under
619 chapter 258F.