SENATE DOCKET, NO. 1028 FILED ON: 1/15/2015

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

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

SENATE DOCKET, NO. 1028 FILED ON: 1/15/2015

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:

SECTION 1. Section 37E of chapter 266 of the General Laws, as appearing in the 2012 Official Edition, is hereby amended by inserting before the definition “Harass” the following definition:-

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

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

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

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

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

"Law enforcement agency", any law enforcement organizations of the Commonwealth, or any of its political subdivisions.

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

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

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

(2) the judgment of conviction; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(iv) Additional relief the court deems necessary.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(i) is not a public record; and

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

(6) The attorney general shall adopt regulations to carry out the provisions of this section. The regulations must include a procedure by which the Office of the attorney general is

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

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

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

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

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

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

“Computer software”, a sequence of instructions written in any programming language that is executed on a computer.

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

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

"Damage" means any significant impairment to the integrity or availability of data, software, a system, or information.

"Execute," when used with respect to computer software, means the performance of the functions or the carrying out of the instructions of the computer software.

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

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

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

"Person", any natural person, business, or state or local agency or political subdivision.

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

"Reencoder", an electronic device that places encoded information from the magnetic strip or stripe of a payment card on to the magnetic strip or stripe of a payment card on to the magnetic strip or stripe of a different payment card.

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

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

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

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

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

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

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

(ii) modify computer or Internet settings;

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

(A) falsely representing that software has been disabled.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(d) Law enforcement agencies shall:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

"Document-making device", an implement, tool, equipment, impression, laminate, card, template, computer file, computer disk, electronic device, hologram, laminate machine or computer hardware or software.

"Password" or "personal identification number", a unique and random number or a unique and random combination of numbers, letters or symbols.

"Person", natural person, corporation, association, state or local agency or political subdivision, partnership or other legal entity.

"Social security number", the nine digit number assigned by the federal government as a method to account for an individual's taxable earnings.

(b) No person shall:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(i) a signed Identity Theft affidavit;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(Date and Place) (Signature)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CHAPTER 258F.

RELIEF FOR IDENTITY THEFT VICTIMS

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

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

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

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

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

"Person", natural person.

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

(1) the arrest warrant;

(2) the complaint

(3) the indictment; and

(4) the judgment of conviction.

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

(1) The petitioner shall state:

(i) the petitioner's full name;

(ii) the petitioner's date of birth;

(iii) the petitioner's address;

(iv) the specific criminal charge to be expunged;

(v) the date of the arrest;

(vi) the name of the arresting agency

(vii) the date of final disposition of the charge as set forth in the petition; and

(viii) the full name used by the thief at the time of arrest.

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

(i) the identity theft report;

(ii) the identity theft passport;

(iii) the identity theft affidavit;

(iv) a copy of the complaint;

(v) a copy of the warrant;

(vi) a copy of the indictment;

(vii) the judgment of conviction; and

(viii) any other information ordered to be part of the record by the court.

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

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

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

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

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

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