HOUSE DOCKET, NO. 3618 FILED ON: 1/20/2017

HOUSE . . . . . No. 2814

The Commonwealth of Massachusetts

PRESENTED BY:

James M. Cantwell

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 addressing cybercrime through enhanced criminal penalties, civil remedies, and transparency.

PETITION OF:

NAME:	DISTRICT/ADDRESS:
James M. Cantwell	*4th Plymouth*
Brian M. Ashe	*2nd Hampden*
Bruce J. Ayers	*1st Norfolk*
Thomas J. Calter	*12th Plymouth*
Tackey Chan	*2nd Norfolk*
Josh S. Cutler	*6th Plymouth*
David F. DeCoste	*5th Plymouth*
Angelo L. D'Emilia	*8th Plymouth*
Shawn Dooley	*9th Norfolk*
Michelle M. DuBois	*10th Plymouth*
Peter J. Durant	*6th Worcester*
Lori A. Ehrlich	*8th Essex*
Denise C. Garlick	*13th Norfolk*
Susan Williams Gifford	*2nd Plymouth*
Paul R. Heroux	*2nd Bristol*
Steven S. Howitt	*4th Bristol*
Kevin J. Kuros	*8th Worcester*

David Paul Linsky	*5th Middlesex*
Rady Mom	*18th Middlesex*
Mathew Muratore	*1st Plymouth*
Patrick M. O'Connor	*Plymouth and Norfolk*
Keiko M. Orrall	*12th Bristol*
Angelo J. Puppolo, Jr.	*12th Hampden*
Richard J. Ross	*Norfolk, Bristol and Middlesex*
Bruce E. Tarr	*First Essex and Middlesex*
Bud Williams	*11th Hampden*

HOUSE DOCKET, NO. 3618 FILED ON: 1/20/2017

HOUSE . . . . . No. 2814

By Mr. Cantwell of Marshfield, a petition (accompanied by bill, House, No. 2814) of James M. Cantwell and others relative to amending certain statutes pertaining to data security breaches and calling for an investigation by a special commission (including members of the General Court) on cybersecurity to assess the various threats across the Commonwealth. Consumer Protection and Professional Licensure.

The Commonwealth of Massachusetts

In the One Hundred and Ninetieth General Court
(2017-2018)

An Act addressing cybercrime through enhanced criminal penalties, civil remedies, and transparency.

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 6 of chapter 93H of the General Laws, as appearing in the 2014 Official Edition, is hereby further amended, in line 1, by inserting before the word “The” the following letter:-(a).

SECTION 2. Section 6 of said chapter 93H, as so appearing, is hereby further amended by inserting, after paragraph (a), the following paragraphs:-

(b) Any person or agency that owns or licenses the data shall not be liable for damages from a security breach when: (1) the data owner or licensor is in compliance with this chapter; and (2) the security breach was not the result of intentional misconduct or the negligence of the data licensor, its agents, or employees. Any person who has been injured by a security breach may bring a civil action for actual damages, reasonable attorney’s fees, and court costs.

(c) Any person or agency that owns or licenses data, that provides the requisite notice to comply with section 3, may bring a civil action against a person that unlawfully obtained or negligently benefited from information maintained by the data owner or licensor, for actual damages, reasonable attorney's fees, court costs, and the reasonable costs of notification.

(d) Remedies provided by this chapter are cumulative and do not affect the availability of remedies under other law.

SECTION 3. (a) There shall be a special commission on cybersecurity, pursuant to section 2A of chapter 4 of the General Laws, to assess the various cybersecurity threats across the commonwealth and to recommend corresponding legislative action, risk-management strategies, and response plans.

The special commission shall:

(1) promote the prevention of cybercrime, the enforcement of cybersecurity laws, the investigation and prosecution of cyber criminals, and the destruction of cybercrime enterprises, including through improved collaboration among local, state, and federal law enforcement across national and international jurisdictions;

(2) assess cybersecurity threats facing persons, agencies, organizations, and corporations in the Commonwealth;

(3) assess deficiencies in current preventative risk-management plans and the existing laws intended to safeguard public and personal information and respond to cybercrime;

(4) assess deficiencies in the laws governing cybersecurity breach response plans and response notification requirements;

(5) recommend strategies, including legislative action, to promote cybersecurity, deter cybercrime, and promote robust data security;

(6) recommend programs and practices to improve and incentivize preventative risk-management plans; and

(7) recommend strategies, including legislation, to improve data security against cyber threats without unduly burdening data storing entities;

The commission shall consist of 18 members or their designees: 2 members of the house of representatives, 1 of whom shall be appointed by the speaker of the house and shall serve as co-chair, and 1 of whom shall be appointed by the minority leader of the house of representatives; 2 members of the senate, 1 of whom shall be appointed by the senate president and shall serve as co-chair, and 1 of whom shall be appointed by the minority leader of the senate; the attorney general; the treasurer; the secretary of public safety and security; the superintendent of the state police; the secretary of the executive office of housing and economic development; secretary of the executive office of health and human services; the commissioner of the department of public utilities; the executive director of the health connector; the assistant secretary for masshealth; and 5 members who shall be appointed by the governor, 1 of whom shall be an expert in commercial cybersecurity, 1 of whom shall be an expert in public infrastructure cybersecurity, 1 of whom shall be a legal expert in high technology and cybercrime, 1 of whom shall be a law enforcement officer in cybercrime, and 1 of whom shall be an expert in data security or computer engineering.

The commission may hold public meetings and fact-finding hearings as it considers necessary; provided, however, that the commission shall conduct at least 3 public hearings to

receive testimony from members of the public and experts. The commission shall file the report of its study with the governor and the clerks for the house of representatives and the senate.

SECTION 4. Section 1 of chapter 93H of the General Laws, as appearing in the 2014 Official Edition, is hereby amended by striking out said section and inserting in place thereof the following section:-

Section 1. (a) As used in this chapter, the following words shall, unless the context clearly requires otherwise, have the following meanings:

"Access device", a card issued by a financial institution that contains a magnetic stripe, microprocessor chip, or other means for storage of information which includes, but is not limited to, a credit card, debit card, or stored value card.

“Agency”, any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or any of its branches, or of any political subdivision thereof.

“Biometric indicator”, any unique biological attribute or measurement that can be used to authenticate the identity of an individual, including but not limited to fingerprints, genetic information, iris or retina patterns, facial characteristics, or hand geometry.

“Breach of security”, the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates an identifiable risk of identity theft or fraud. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the

personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

“Data”, any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

“Encrypted”, transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, unless further defined by regulation of the department of consumer affairs and business regulation.

"Financial institution", any office of a trust company, commercial bank, industrial loan company, savings bank, savings and loan association, cooperative bank or credit union chartered by the commonwealth or by another state of the United States, the District of Columbia, the commonwealth of Puerto Rico, a territory of possession of the United States, or a country other than the United States, or a national banking association, federal savings and loan association, federal savings bank or federal credit union.

“Information security program”, the administrative, technical, or physical safeguards that a covered entity uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personal information.

“Notice”, shall include:

(i) written notice;

(ii) electronic notice, if notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 (c) of Title 15 of the United States Code; and chapter 110G; or

(iii) substitute notice, if the person or agency required to provide notice demonstrates that the cost of providing written notice will exceed $250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person or agency does not have sufficient contact information to provide notice.

“Person”, a natural person, corporation, association, partnership or other legal entity.

“Personal information”, a resident’s first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident:

(a) Social Security number;

(b) driver’s license number or state-issued identification card number;

(c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident’s financial account; or

(d) biometric indicator; provided, however, that “Personal information” shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

"Service provider", a person or entity that stores, processes, or transmits access device data on behalf of another person or entity.

"Substitute notice", shall consist of all of the following:

(i) electronic mail notice, if the person or agency has electronic mail addresses for the members of the affected class of Massachusetts residents;

(ii) clear and conspicuous posting of the notice on the home page of the person or agency if the person or agency maintains a website; and

(iii) publication in or broadcast through media or medium that provides notice throughout the commonwealth.

(b) The department of consumer affairs and business regulation may adopt regulations, from time to time, to revise the definition of "encrypted", as used in this chapter, to reflect applicable technological advancements.

SECTION 5. Section 2 of said chapter 93H is hereby further amended by striking out the first paragraph and inserting in place thereof the following paragraphs:-

Section 2. (a) The department of consumer affairs and business regulation shall adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth. Such regulations shall require a person subject to this chapter to develop, implement, and maintain a comprehensive information security program that contains administrative, technical, and physical safeguards that are reasonably designed to (1) ensure the security and confidentiality of personal information of residents of the commonwealth, (2) protect against any anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized acquisition of such information that could result in substantial harm to the individuals to whom such information relates.

The regulations shall require a person subject to this chapter to (1) designate an employee or employees to coordinate the information security program, (2) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of sensitive financial account information and sensitive personal information and assess the sufficiency of any safeguards in place to control these risks, including consideration of risks in each relevant area of the covered entity's operations, (3) design and implement information safeguards to control the risks identified in its risk assessment, and regularly assess the effectiveness of the safeguards' key controls, systems, and procedures, and (4) oversee third-party service providers by taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate safeguards for personal information and requiring third-party service providers by contract to implement and maintain such safeguards.

A person shall be deemed to be in compliance with this chapter if it is subject to 15 U.S.C. 6801, 42 U.S.C. 1320d–2, or 42 U.S.C. 17932 and 17937 and the regulations promulgated under these sections.

SECTION 6. Section 3 of said chapter 93H is hereby further amended by striking out the third paragraph and inserting in place thereof the following paragraph:-

The notice to be provided to the resident shall include, but not be limited to, the consumer's right to obtain a police report, how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze, and any fees required to be paid to any of the consumer reporting agencies.

SECTION 7. Chapter 266 of the General Laws is hereby amended by striking out section 33A, as so appearing, and inserting in place thereof the following section:-

Section 33A. (a) Whoever, with intent to defraud, obtains, or attempts to obtain, or aids or abets another in obtaining, any public or commercial computer service by false representation, false statement, unauthorized charging to the account of another, by installing or tampering with any facilities or equipment or by any other means, shall be guilty of obtaining computer services by fraud or misrepresentation, and shall, if resulting in damages that do not exceed five thousand dollars, be punished for a first offense by imprisonment in the house of correction for not more than two and one-half years or by a fine of not more than three thousand dollars, or both, and for a subsequent offense, by imprisonment for not less than one year nor more than two and one half years, or by a fine of not less than three hundred nor more than three thousand dollars, or both; or, if as a result of such, (1) damages exceed five thousand dollars, (2) endangers human life, (3) cause serious injury, (4) disrupts a computer service for public safety, healthcare, energy infrastructure, or (5) disrupts a computer service that affects medical equipment used for the direct administration of medical care or treatment to a person, shall be punished by imprisonment in the house of correction for not more than five years or by a fine of not more than twenty-five thousand dollars, or both, and for a second offense by imprisonment in the house of correction for not less than two and one half years nor more than five years, or by a fine of not less than two thousand and five hundred nor more than twenty-five thousand dollars, or both.

(b) As used in this section, the words "public and commercial computer service" shall mean the use of computers, computer systems, computer programs or computer networks, or the access to or copying of the data, where such use, access or copying is: (1) administered by any local or state government; or (2) offered by the proprietor or operator of the computer, system, program, network or data to others on a subscription or other basis for monetary consideration.

SECTION 8. Section 120F of Chapter 266 of the General Laws, as appearing in the 2014 Official Edition, is hereby amended, in line 5, by striking the words “thirty days”, and inserting in place thereof the following words:- six months

SECTION 9. Section 120F of Chapter 266 of the General Laws, as appearing, is hereby amended, in line 6, by striking the word “both.”, inserting in place thereof the following words:- both; or, if such access includes the system’s camera, microphone, or location services, shall be punished by imprisonment in the house of correction for not more than one year or by a fine of not more than five thousand dollars, or both; or, if access or, if as a result of such access, (1) damages exceed five thousand dollars, (2) endangers human life, (3) cause serious injury, or (4) disrupts a computer service that affects medical equipment used for the administration of medical care or treatment to a person, shall be punished by imprisonment in the house of correction for not more than five years or by a fine of not more than twenty-five thousand dollars, or both.

SECTION 10. Chapter 266 of the General Laws, as appearing, is hereby amended by inserting after section 120F the following section:-

Section 120G. Whoever, intentionally interferes with, denies or causes the denial of access to or use of a computer, system, or network to an authorized user of a computer system, shall be punished by imprisonment in the house of correction for not more than one year or by a fine of not more than five thousand dollars, or both; or, if such interference denies, interrupts, impairs, or causes the denial of access to or use of a public safety or healthcare infrastructure computer system, shall be punished by imprisonment in the house of correction for not less than

one year and not more than two and one half years, or by a fine of not less than one thousand dollars and not more than ten thousand dollars, or both.