THE COMMONWEALTH OF MASSACHUSETTS
OFFICE OF THE ATTORNEY GENERAL
ONE ASHBURTON PLACE
BOSTON, MASSACHUSETTS 02108

MAURA HEALEY
ATTORNEY GENERAL

(617) 727-2200
(617) 727-4765 TTY
www.mass.gov/ago

Prepared Statement of Sara Cable
Assistant Attorney General and Director of Data Privacy & Security
Consumer Protection Division
Office of the Massachusetts Attorney General

Before the House of Representatives
Subcommittee on Financial Institutions and Consumer Credit

Hearing Entitled "Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime"

March 7, 2018

Introduction

Chairman Luetkemeyer, Ranking Member Clay, and members of the Subcommittee, thank you for inviting me to testify today regarding the discussion draft bill, entitled the Data Acquisition and Technology Accountability and Security Act, dated February 16, 2018 (the "Bill"). I am an Assistant Attorney General for the Massachusetts Attorney General's Office, and the Director of Data Privacy and Security for its Consumer Protection Division. On behalf of the Office, I appreciate the opportunity to share our experience over the past decade enforcing the Massachusetts Data Breach Notice Law and Data Security Regulations (Mass. Gen. Laws c. 93H; 201 CMR 17.00 *et seq.*).

We applaud the Subcommittee's recognition of the importance of strong data security protections and breach disclosure obligations. It seems every day consumers learn of a new data breach at yet another well-known company: TJX, Sony, Adobe, Target, Home Depot, Yahoo!, Anthem, Uber, and Equifax, just to name a few. These occurrences seem so common, they feel inevitable, a sentiment encapsulated by the oft-stated warning of cybersecurity professionals: "it is not a question of whether a breach will happen, but when."

The recent news of the Equifax breach—which put 145.5 million Americans at risk of identity theft and financial fraud—has once again brought this issue to the forefront of the public consciousness. Equifax may be the latest massive breach, but if history is any guide, it will not be the last. That a company in the very business of safeguarding and managing vast troves of the most sensitive consumer data failed to protect it despite knowing that its systems were vulnerable

to hackers makes clear that more must be done to protect consumers and preserve their confidence in the market.

Now is not the time to dilute or preempt the tools regularly and successfully used by many states, including Massachusetts, to combat this crisis. Especially in light of breaches like Equifax, this is the time to build on and improve existing protections under federal and state law. This Subcommittee's first priority should be protecting consumers from the dangers posed by data breaches, not minimizing compliance costs for businesses that allow breaches to occur. Congress should not expose American consumers to increased risks as a result of a new, less stringent national standard.

For the past decade, the Massachusetts Attorney General's Office, along with its sister States, have been on the front lines on this cybersecurity problem. We help consumers in the aftermath of a breach as they struggle to protect themselves from identity theft, fraud, or other harms. We engage with business on a regular basis, providing guidance on compliance with the Massachusetts Data Breach Notice Law and Data Security Regulations, and educating them on emerging cybersecurity threats and strategies to avoid them. And through the Massachusetts Consumer Protection Act and Data Breach Notification Law, we hold companies accountable when they fail to comply with our law and keep consumers' data safe from foreseeable threats.

As the "cop on the beat" working on the front lines of the data security problem, we believe that this Bill, taken as a whole, will leave consumers in a worse position than the status quo. As I will describe below, this Bill allows entities to push the cost of the data security crisis onto consumers without providing any meaningful remedy, strips the state Attorneys General of the authority they are presently and actively using to protect their consumers from breaches, and hamstrings efforts of the States to enact laws in response to future risks in an era of increasing and rapidly evolving technology.

Discussion

I. The Bill Makes It Harder for State Attorneys General—the "Cops on the Beat"—to Do Their Jobs.

a. Direct Notice to State Regulators Is Essential.

The Massachusetts Data Breach Notice Law and Data Security Regulations are recognized as among the strongest in the nation. Together, they protect consumers by requiring entities that own or license "personal information"[1] of Massachusetts residents to develop, implement, and maintain minimum security safeguards to protect such information from foreseeable threats and from unauthorized access or use.[2] If such information is breached,

[1] In Massachusetts, "personal information" is defined as a resident's first name and last name, or first initial and last name, in combination with any one or more of the following data elements: (a) social security number; (b) driver's license number or state-issued identification card number; or (c) financial account number or credit or debit card number, with or without any required security code. *See* Mass. Gen. Laws. c. 93H, §1 (**Exhibit 1**).

[2] *See* Mass. Gen. Laws c. 93H (the Massachusetts Data Breach Notice Law); 201 C.M.R. 17.00 *et seq.* ("Standards for the Protection of Personal Information of Residents of the Commonwealth") (the Massachusetts Data Security Regulations), and Mass. Gen. Laws. c. 93I (the Massachusetts Data Disposal Law) (**Exhibits 1–3**).

Massachusetts law obligates entities to notify, "as soon as practicable and without unreasonable delay" each affected resident, as well as other state agencies, including the Attorney General.[3]

Over the last decade, over 21,000 data breaches have been reported to our Office under the Massachusetts Data Breach Notice law, and over ten million data breach notifications have been sent to Massachusetts consumers. In 2017 alone, over 3,800 breaches were reported to our Office. Direct notice of breaches to our Office is a critical component of our law. It allows us to ensure that consumers are promptly and properly notified so that they can take steps to protect themselves from resulting identity theft or fraud. Direct notice also allows us to engage in education and outreach to the business community to increase awareness of the importance of data security. Finally, it gives our Office an informed and comprehensive view into the nature, extent, and frequency of breaches, the risks faced by consumers, and the security practices and procedures that can prevent or mitigate those risks.

As currently drafted, the Bill unwisely does away with direct notice of breaches to state Attorneys General for those breaches that impact their residents. This is in direct contrast to the current requirements under Massachusetts Law, and the laws of twenty-four other states.[4] Such a change to the status quo would directly and significantly impact our ability to protect our residents. In the absence of direct notice, any given state Attorney General instead would have to rely on individual consumers, media, or whistleblowers to bring breaches to their attention, an impractical approach that forces a state Attorney General Office to navigate delays and unnecessary burdens to obtain information about the overall scope of a breach and its impact on state residents. A better solution that also promotes the interests of consumers is to require entities to directly notify state Attorneys General of breaches impacting their state's residents, as many state laws already require.

In addition, the Bill's proposed threshold for notice to federal regulators (breaches that impact 5,000 or more consumers of any state) is likely not to capture the vast majority breaches that, while not nationally significant in size, may have a significant impact on the residents of a particular state. For example, in Massachusetts, *less than 1%* of the over 3,800 data breaches reported to our Office in 2017 impacted 5,000 or more Massachusetts consumers. Indeed, over 93% of the over 3,800 breaches impacted fewer than 100 residents each. Assuming similar statistics in other states, the Bill risks creating an enforcement "blind spot" for both state and federal regulators, who would not receive notice of the vast majority of data breaches that occur. While such thresholds may work for large breaches that affect consumers nationwide, it does not work for breaches that affect only one state or region.

---

[3] *See* Mass. Gen. Laws c. 93H, § 3(b) (**Exhibit 1**).

[4] *See* Cal Civ. Code § 1798.82; Conn. Gen. Stat. § 36a-701b; Fla. Stat. § 501.171; H.R.S. § 487N-1 *et seq*; Idaho Code § 28-51-104 *et seq*.; Iowa Code § 715C.1-2; La. Rev. Stat. § 51:3071 *et seq*; 10 Me. Rev. Stat. § 1346 *et seq*.; Md. Code Com. Law § 14-3501 *et seq*.; Mass. Gen. Laws c. 93H § 3(b); Mo. Rev. Stat. § 407.1500; Mont. Code § 30-14-1701 *et seq*.; Neb. Rev. Stat. § 87-801 *et seq*.; N.H. Rev. Stat. § 359-C:19 *et seq*; N.J. Stat. § 56:8-163; [NM] H.B. 15 (signed into law April 6, 2017); N.Y. Gen. Bus. Law § 899-aa; N.C. Gen. Stat. §§ 75-61, 75-65; N.D. Cent. Code § 51-30-01 *et seq*.; Or. Rev. Stat. §§ 646A.604; R.I. Gen. Laws § 11-49.2-1 *et seq*.; S.C. Code § 39-1-90; 9 V.S.A. §§ 2430, 2435; Va. Code § 18.2-186.6; and Wash. Rev. Code § 19.255.010 *et seq*.

b. The Bill's Enforcement Mechanisms (Section 5) Hinder the States' Ability to Protect Their Consumers.

Also critical to our consumer protection efforts is our authority to investigate the circumstances of data breaches, and where appropriate, enforce the Massachusetts Data Breach Notice Law and Data Security Regulations. This authority derives primarily from the Massachusetts Consumer Protection Law (Mass. Gen. Laws c. 93A). We do so in situations where the circumstances of a breach reflect gross failures by an entity to implement or maintain basic security practices, where the entity unreasonably delayed providing notice of the breach, or other egregious conduct that raises real risks of resulting consumer harm. This enforcement authority allows us to obtain restitution for those consumers who suffered ascertainable losses, and deter wrongdoing by companies in the future through civil penalties and injunctive relief.

For example, on September 19, 2017, this Office filed suit against Equifax under our Consumer Protection and Data Breach Notice laws for its conduct in leaving the personal information of three million Massachusetts residents vulnerable to hackers, despite knowing for months that its website was insecure. Among other things, we allege that Equifax violated the Massachusetts Consumer Protection Act and Data Security Regulations, which require Equifax to develop, implement, and maintain reasonable administrative, technological, and physical safeguards to protect consumers' data from foreseeable harm. We also allege that Equifax failed to promptly notify consumers that their information was compromised, in violation of the Massachusetts Data Breach Notice Law, and that it compounded consumers' harm, including by charging consumers to implement security freezes necessitated by its own mistakes. In our view, Equifax could have prevented this breach, and it must be held accountable for failing to do so.[5]

The enforcement provisions contemplated by the Bill (Section 5) significantly infringe on this Office's enforcement powers to consumers' detriment. Although state Attorneys General have been the "cops on the beat" of the data security problem for the past decade,[6] the Bill shifts primary enforcement authority from the States to the federal government. In our view, this would hamper the effectiveness of a federal law with respect to data breach notification and data security. Too many breaches occur for any one agency to respond effectively to all of them. Some breaches will be too small to be a priority at the federal level, yet such breaches could have a large impact in a particular state or region.

The Bill also erects procedural hurdles that further burden the States and infringe on their enforcement powers and prerogatives. While the Bill gives the state Attorneys General the option of bringing a civil action as *parens patriae* in U.S. district court, it requires the State to first notify the FTC, and to abstain if the FTC initiates action first. It further allows the FTC to intervene in pending cases, and requires the consolidation of cases by different states into the U.S. District Court for the District of Columbia without regard to the locus of any of the parties. Such requirements inject delay and costs onto the States, unnecessarily complicating their enforcement efforts. Dual federal/state enforcement coordination of consumer protection laws

[5] A copy of our Complaint is attached as **Exhibit 4**.

[6] *See generally*, Danielle K. Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2017), *available at* https://scholarship.law.nd.edu/ndlr/vol92/iss2/5.

without such burdens is both possible and effective.[7] To ensure meaningful protections for consumers, the Bill should likewise establish a dual federal/state enforcement framework that respects—not constricts—the enforcement prerogative and agility of the States.

Finally, we note with particular concern the provisions of this Bill that appear to foreclose the States' ability to sue "financial institutions"—even in the face of the institution's knowing failures to protect consumers' data. *See* Section 5(b)(5). Our consumers rely on financial institutions to protect their most sensitive, personal information. An institution's failure to implement reasonable data security safeguards to protect that information from a foreseeable breach represents a shocking betrayal of public trust, and poses an unacceptable risk to our consumers. This Bill prevents our Office, and all states, from discharging our duties to protect our consumers. There is no justification—especially in light of Equifax—for such a drastic rollback of the States' enforcement powers.

II. The Bill Leaves Consumers in a Worse Position than the Status Quo.

a. The Bill's Breach Notice Requirements (Section 4) Will Not Protect Consumers from Identity Theft, Financial Losses, or Other Harms.

If preventing identity theft and consumer harm is the goal of a data breach notice regime, requiring notice of the breach to the consumer as soon as possible must be the first priority. One study found that the breach of a Social Security number increases a consumer's risk of identity theft by 18 times.[8] Breaches of information such as email addresses, phone numbers, or other identifying information also subject the consumer to increased risks of scams, phishing, or other fraud. Prompt consumer notification allows consumers the opportunity take proactive steps to protect themselves from identity theft, financial fraud, or other harm before it occurs. Conversely, delayed notice increases the risk of harm by shortening or eliminating the window of opportunity for such prophylactic steps.

Public notice of a data breach also serves an important deterrent purpose. Having to notify customers of data security lapses creates a powerful incentive for a company to improve its data security practices to avoid a breach.

The consumer notification standards under this Bill (Section 4) do not achieve these goals. The Bill only requires consumer notice if the entity "determines after completion of [its] preliminary investigation … that there is a reasonable risk that the breach … *has resulted* in identity theft, fraud or economic loss…." *See* Section 4(b)(2). In other words, contrary to today's regime under most state laws (where consumers are notified of breaches that raise the risks of *future* identity theft, fraud or economic loss), consumers would not be notified until *after that risk has manifested in harm*. This unacceptably externalizes the costs of a company's poor

[7] See, for example, the Federal Trade Commission Act (15 U.S.C. 45(a)(1) and its numerous state counterparts (*see, e.g.* Mass Gen. Laws c. 93A), and the Health Insurance Portability and Accountability Act (HIPAA) (Pub. L. No. 104-191, 110 Stat. 1936 (1996)) and the Health Information Technology for Clinical and Economic Health (HITECH) Act (42 U.S.C. 17930 *et seq*.).

[8] National Consumers League, The Consumer Data Insecurity Report: examining the Data Breach – Identity Fraud Paradigm in Four Major Metropolitan Areas, 14, (June 2014).

security practices onto consumers, an outcome especially unfair given that there is no clear authority to state Attorneys General to obtain restitution for such consumers. It also deprives the consumer of the ability to make his or her own determination of risk and take those steps he or she deems appropriate to mitigate it.

Further, by allowing the entity to determine whether or not consumers suffered harm before providing consumer notice, the Bill creates clear opportunities for abuse. Connecting any specific breach to identity theft or financial harm, or tracing identity theft to any particular breach over another, can be a difficult and time consuming process, and in practice, may be impossible. Because the Bill does not require the covered entity to conduct such an investigation,[9] a covered entity might opt to avoid this expense. Finally, the Bill does not take into account non-financial harms that can occur from a data breach about which consumers should be notified, such as professional or personal embarrassment,[10] or loss of access to online accounts or services.

Additionally, by requiring covered entities to conduct a preliminary investigation based on its own belief (reasonable or not) "that a breach of security containing personal information may have occurred," without also imposing an outer time limit on that investigation risks injecting even further delay in the notification timeline. A federal standard should instead require breach notification as soon as reasonably practicable and without unreasonable delay when an entity knows, or has reason to know, that protected personal information of a consumer has been acquired without authorization, or used for unauthorized purposes.

Finally, the distinction drawn in the Bill between "covered entities" and "third parties" for purposes of notification (Section 4(c)) creates opportunities for delay as a result of disputes between covered entities as to which is the "third-party entity" and which is ultimately responsible for notice.[11] To ensure consumers are notified, Massachusetts imposes notification obligations based on the entity's legal relationship to the breached personal information.[12]

---

[9] *Compare* Section 4(a)(3) (requiring a covered entity to conduct a preliminary investigation based on its belief (reasonable or not) "that a breach of security containing personal information may have occurred," to, among other things, "determine if the personal information has or is likely to have been acquired without authorization.").

[10] *See* Stipulated Order for Permanent Injunction and Other Equitable Relief, *FTC v. Ruby Corp., Ruby Life Inc., dba AshleyMadison.com, and ADL Media Inc.*, Case No. :16-cv-02438 (D.D.C. Dec. 14, 2016) (resolving FTC complaint alleging that operators of adult dating website had lax data security practices contrary to promises of privacy and security made to consumers, resulting in a data breach in August of 2015 and the publication by hackers of the sensitive profile, account security, and billing information for more than 36 million users).

[11] The Bill imposes the consumer notice obligation on "a covered entity" that "accesses, maintains, or stores personal, or handles personal information," (Sections 2(7) and 4(b)(2)) but not on the "third party" entity that "processe[s], maintain[s], stores, or handles, or otherwise is permitted access to personal information in connection with providing services to a covered entity" (Section 2(11)(A)).

[12] *See* Mass Gen. Laws c. 93H, §§ 3(a), (b) (entities that "maintain or store, but do[] not own or license data" are obligated to promptly notify the owner or licensor, which are the entities that bear the ultimate duty to notify the consumers and state agencies).

b. The Bill Does Not Allow States to Adequately Redress Consumers' Losses.

Data breaches cause real harm to consumers. Armed with an individual's sensitive and personal information—including in particular a Social Security number, date of birth, and/or a drivers' license number—a criminal can commit identity theft, financial fraud, and other identity-related crimes. Identity theft results in real financial losses, loss of access to credit and even essential services like utilities, and fear and anxiety for consumers.[13] Even if identity theft never occurs, victims of a data breach must spend time and money to protect themselves from future harm. Recommended measures include placing security freezes or fraud alerts, purchasing credit monitoring services, scrutinizing financial accounts and obtaining new account numbers, identification documents, or credentials, among other efforts.

Despite requiring entities to notify consumers only in circumstances where those consumers have suffered financial harm, the Bill does not authorize their state's Attorney General to obtain damages for that harm (and appears to preempt any state law, such as the Massachusetts Consumer Protection Act, that might allow for such a remedy). Rather, state Attorneys General would be limited to seeking civil penalties and injunctive relief, even in cases where consumers suffer extensive harm as a result of a breach of highly sensitive information. As a result, and again, the Bill unacceptably passes the consequences of data breaches onto consumers. We urge the Committee not to preempt and displace the existing authority of state law enforcement to make their residents whole.

c. The Proposed "Security Safeguards" (Section 3) Should Be at Least as Strong as Existing Federal and State Standards.

The Subcommittee rightly recognizes that minimum data security standards are essential to protect consumers and businesses alike from data breaches. Indeed, our review of thousands of breach notifications underscores the importance of strong, and enforceable, data security standards. While some breaches result from intentional, criminal acts, many result from the failure to employ basic security practices, such as the improper disposal of consumers' information, lost files, disclosure through inadvertence, carelessness, or the failure to follow basic and well-accepted data security practices. Often even those breaches resulting from intentional criminal attacks could reasonably have been avoided or mitigated if the entity had complied with its own data security policies or employed basic security practices such as deploying software updates, patches, or firewalls.

Massachusetts has had robust minimum data security regulations in place since 2010 in the form of its Data Security Regulations (201 CMR 17.00 *et seq.*) and its Data Disposal Law (Mass Gen. Laws c. 93I). In our view, the flexible but strong minimum standards established by

[13] In its 2014 Victims of Identity Theft report, the United States Department of Justice stated that 65% of the over 17 million identity theft victims that year suffered a financial loss, and 13% of the total identity theft victims never had those losses reimbursed. *See* U.S. Dept. of Justice, Bureau of Justice Statistics, Victims of Identity Theft 2014, at 6 & Table 6, *available at* http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408. The average out-of-pocket loss for those victims was $2,895. Identity theft victims also "paid higher interest rates on credit cards, they were turned down for loans or other credit, their utilities were turned off, or they were the subject of criminal proceedings." *Id*. at 8. With respect to consumers' emotional distress, the report also noted that more than one-third of identity theft victims were moderately or severely distressed due to the crime. *See id*. at 9, Table 9.

Massachusetts represent the leading, generally-applicable information security framework in the nation. Rather than employing a "one-size-fits-all" approach, Massachusetts utilizes a risk-based, process-oriented approach to data security, similar to well-established federal standards governing financial institutions and certain health-related entities.[14]

While Section 3 proposes a similar risk-based and flexible framework, it omits several key elements that, in our view, are necessary to ensure they are effective and enforceable. For example, both Massachusetts law and the FTC Safeguards Rule require entities to document their administrative, technical and physical safeguards, and update those policies as necessary.[15] Such written information security programs are critical in ensuring that an entity develops, implements, and maintains a comprehensive and enforceable safeguards. The Subcommittee should also consider requiring entities that suffer a breach to document remedial actions and conduct post-incident reviews.

As to vendor management, the Bill is too lenient. Both the FTC Safeguards Rule and the Massachusetts Data Security Regulations require reasonable oversight of third party service providers. Massachusetts requires entities to "[o]versee service providers, by: 1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with these regulations and any applicable federal regulations; and 2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information." 201 CMR 17.03(2)(f). The FTC Safeguards Rule has a similar requirement. *See* 16 CFR § 314.4(d). By contrast, the Bill requires covered entities merely to "maintain reasonable procedures for the security of personal information by third parties" (Section 3(a)(3)(D)). In our experience, more robust third party oversight is necessary to prevent entities from outsourcing their responsibility to protect their customers' data.

Finally, Section 3 does not define or enumerate any examples of the required "reasonable safeguards" that an entity must maintain, or provide any agency with rule-making authority to do so. For example, although the Bill generally contemplates that entities will maintain some form of computer and network system security, *see* Section 3(a)(3)(B)(ii), it does not specify what safeguards should be encompassed by that system. By contrast, both Massachusetts Law and the HIPAA Security Rule specify the various technical safeguards each requires, such as: secure

---

[14] Massachusetts law requires covered entities to develop, implement, and maintain a written security program outlining administrative, technological, and physical safeguards appropriate for the entity's size, scope of business, amount of resources available to it, the nature and quantity of data collected or stored, and the need for security of the personal information it handles. Within this flexible and technology-neutral framework, the regulations outline various categories of minimum security measures. *See generally,* **Exhibit 2** (201 CMR 17.00 *et seq.*). In this way, Massachusetts is similar to federal law governing financial institutions and health care information. *See* 16 C.F.R. Part 314 (Standards for Safeguarding Customer Information) and 45 CFR Part 160 and Subparts A and C of Part 164 (Security Standards for the Protection of Electronic Protected Health Information).

[15] *See* 201 CMR 17.03(1) ("Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards…); 16 CFR § 314.3(a) ("You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains the administrative, technical, and physical safeguards…"); 45 CFR § 164.316 (Policies and procedures and documentation requirements).

access control and user authentication procedures and mechanisms[16]; encryption of personal information sent over public networks or wirelessly, or stored on laptops and portable devices[17]; network security, such as up-to-date firewall protection and operating system security patches, and system security agent software[18]; and mechanisms to monitor computer systems for unauthorized use of or access to personal information.[19]

Forcing covered entities to guess what constitutes such "reasonable safeguards" exposes them to litigation risks, increases compliance uncertainty and costs, and may lead to a downward harmonization towards the least expensive (and likely least effective) measures. Relying on litigation to establish what is "reasonable" also will not keep pace with evolving security threats. For these reasons, we urge the Subcommittee to not override and preempt existing, more stringent state data security protection.

III. The Bill's Proposed Preemption of State Law (Section 6) Will Prevent States from Protecting Their Consumers from Rapidly-Evolving Digital Risks.

Section 6 of the Bill would entirely and wrongly preempt existing state data breach and data security law that provide better protections for consumers. Federal standards should not preempt or undercut stronger provisions of state law, especially in the rapidly evolving space of cybersecurity and data protection. Instead of establishing a national security and breach standard that may fail to keep up with changing technologies, we urge the Subcommittee not to establish a ceiling for data security, but at most a federal "floor" of protections that state law can exceed as necessary to protect their consumers from emerging risks. *See, e.g.*, 15 U.S.C. § 6807(b) (Gramm-Leach-Bliley Act) ("[A] State statute, regulation, order, or interpretation is not inconsistent with this [law] if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this [law] . . . .").

Additionally, the scope of the proposed preemption is unduly broad, covering not only state laws concerning "personal information" but rather, state laws "with respect to securing *information* from unauthorized access or acquisition …." (emphasis added). This could sweep into its scope a multiple of existing state laws, such as state criminal laws concerning

[16] *See, e.g.*, 201 CMR 17.04(1); 45 CFR §§ 164.308(a)(4), (5)(ii)(D); 164.312(a)(1), (2)(i).

[17] *See e.g.*, 201 CMR 17.04(3), (5); 45 CFR § 164.312(a)(2)(iv), (e)(2)(ii).

[18] *See, e.g.*, 201 CMR 17.04(6), (7).

[19] *See, e.g.*, 201 CMR 17.04(4).

unauthorized access to a computer system[20] or the interception of wire communications,[21] or laws protecting medical records and mental health records from unauthorized access.[22]

Such a broad scope could further have a chilling effect on state legislatures, who are increasingly called on to respond to new and evolving security and privacy risks to their residents. In fact, this Office is actively engaged with the Massachusetts Legislature in order to bring additional tools and protections to consumers who are victims of data breaches.[23] The increasing threat and ever-evolving nature of data security risks demands the kind of agility and innovation that states are best positioned to provide. We urge the Subcommittee to respect the important role of the States and instead establish a minimum, not a maximum, standard of federal protection.

Conclusion

Thank you for this opportunity to convey our concerns regarding the Bill to the Subcommittee. Please do not hesitate to contact us for any additional detail, clarity or with questions you may have. We are happy to provide you with any information you may need or to share with you our experience gained from working with businesses, reviewing security breach notifications, and enforcing our laws.

[20] *See* Mass. Gen. Laws c. 266, § 120F ("Whoever, without authorization, knowingly accesses a computer system by any means, or after gaining access to a computer system by any means knows that such access is not authorized and fails to terminate such access, shall be punished by imprisonment in the house of correction for not more than thirty days or by a fine of not more than one thousand dollars, or both. The requirement of a password or other authentication to gain access shall constitute notice that access is limited to authorized users.").

[21] *See* Mass. Gen. Laws c. 272, § 99(C) ("any person who—willfully commits an interception, attempts to commit an interception, or procures any other person to commit an interception or to attempt to commit an interception of any wire or oral communication shall be fined not more than ten thousand dollars, or imprisoned in the state prison for not more than five years, or imprisoned in a jail or house of correction for not more than two and one half years, or both so fined and given one such imprisonment").

[22] *See, e.g.*, Mass Gen. Laws c. 111, § 70E(b), and c. 123, § 36.

[23] *See* S2304, *An Act Relative to Consumer Protection from Security Breaches* (https://malegislature.gov/Bills/190/S2304); H4241, *An Act Removing Fees for Security Freezes and Disclosures of Consumer Credit Reports* (https://malegislature.gov/Bills/190/H4241).

EXHIBIT 1

Massachusetts General Laws Annotated
Part I. Administration of the Government (Ch. 1-182)
Title XV. Regulation of Trade (Ch. 93-110h)
Chapter 93H. Security Breaches (Refs & Annos)

M.G.L.A. 93H § 1

§ 1. Definitions

Effective: October 31, 2007
Currentness

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

“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.

“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 a substantial risk of identity theft or fraud against a resident of the commonwealth. 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.

“Electronic”, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

“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.

“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; or

(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; 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.

“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.

Credits
Added by St.2007, c. 82, § 16, eff. Oct. 31, 2007.

Notes of Decisions (1)

M.G.L.A. 93H § 1, MA ST 93H § 1
Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

Massachusetts General Laws Annotated
Part I. Administration of the Government (Ch. 1-182)
Title XV. Regulation of Trade (Ch. 93-110h)
Chapter 93H. Security Breaches (Refs & Annos)

M.G.L.A. 93H § 2

§ 2. Regulations to safeguard personal information of commonwealth residents

Effective: October 31, 2007
Currentness

(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 be designed to safeguard the personal information of residents of the commonwealth and shall be consistent with the safeguards for protection of personal information set forth in the federal regulations by which the person is regulated. The objectives of the regulations shall be to: insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer. The regulations shall take into account the person's size, scope and type of business, the amount of resources available to such person, the amount of stored data, and the need for security and confidentiality of both consumer and employee information.

(b) The supervisor of records, with the advice and consent of the information technology division to the extent of its jurisdiction to set information technology standards under paragraph (d) of section 4A of chapter 7, shall establish rules or regulations designed to safeguard the personal information of residents of the commonwealth that is owned or licensed. Such rules or regulations shall be applicable to: (1) executive offices and any agencies, departments, boards, commissions and instrumentalities within an executive office; and (2) any authority created by the General Court, and the rules and regulations shall take into account the size, scope and type of services provided thereby, the amount of resources available thereto, the amount of stored data, and the need for security and confidentiality of both consumer and employee information. The objectives of the rules or regulations shall be to: insure the security and confidentiality of personal information; protect against anticipated threats or hazards to the security or integrity of such information; and to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any resident of the commonwealth.

(c) The legislative branch, the judicial branch, the attorney general, the state secretary, the state treasurer and the state auditor shall adopt rules or regulations designed to safeguard the personal information of residents of the commonwealth for their respective departments and shall take into account the size, scope and type of services provided by their departments, the amount of resources available thereto, the amount of stored data, and the need for security and confidentiality of both consumer and employee information. The objectives of the rules or regulations shall be to: insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any resident of the commonwealth.

Credits
Added by St.2007, c. 82, § 16, eff. Oct. 31, 2007.

Notes of Decisions (1)

M.G.L.A. 93H § 2, MA ST 93H § 2
Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

Massachusetts General Laws Annotated
Part I. Administration of the Government (Ch. 1-182)
Title XV. Regulation of Trade (Ch. 93-110h)
Chapter 93H. Security Breaches (Refs & Annos)

M.G.L.A. 93H § 3

§ 3. Duty to report known security breach or unauthorized use of personal information

Effective: October 31, 2007
Currentness

(a) A person or agency that maintains or stores, but does not own or license data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the owner or licensor in accordance with this chapter. In addition to providing notice as provided herein, such person or agency shall cooperate with the owner or licensor of such information. Such cooperation shall include, but not be limited to, informing the owner or licensor of the breach of security or unauthorized acquisition or use, the date or approximate date of such incident and the nature thereof, and any steps the person or agency has taken or plans to take relating to the incident, except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may have been affected by the breach of security or unauthorized acquisition or use. (b) A person or agency that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the attorney general, the director of consumer affairs and business regulation and to such resident, in accordance with this chapter. The notice to be provided to the attorney general and said director, and consumer reporting agencies or state agencies if any, shall include, but not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the commonwealth affected by such incident at the time of notification, and any steps the person or agency has taken or plans to take relating to the incident.

Upon receipt of this notice, the director of consumer affairs and business regulation shall identify any relevant consumer reporting agency or state agency, as deemed appropriate by said director, and forward the names of the identified consumer reporting agencies and state agencies to the notifying person or agency. Such person or agency shall, as soon as practicable and without unreasonable delay, also provide notice, in accordance with this chapter, to the consumer reporting agencies and state agencies identified by the director of consumer affairs and business regulation.

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, provided however, that said notification shall not include the nature of the breach or unauthorized acquisition or use or the number of residents of the commonwealth affected by said breach or unauthorized access or use.

(c) [1] If an agency is within the executive department, it shall provide written notification of the nature and circumstances of the breach or unauthorized acquisition or use to the information technology division and the division of public records as soon as practicable and without unreasonable delay following the discovery of a breach of security or unauthorized acquisition or

use, and shall comply with all policies and procedures adopted by that division pertaining to the reporting and investigation of such an incident.

Credits

Added by St.2007, c. 82, § 16, eff. Oct. 31, 2007.

Notes of Decisions (1)

Footnotes

1 So in original.

M.G.L.A. 93H § 3, MA ST 93H § 3

Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

Massachusetts General Laws Annotated
Part I. Administration of the Government (Ch. 1-182)
Title XV. Regulation of Trade (Ch. 93-110h)
Chapter 93H. Security Breaches (Refs & Annos)

M.G.L.A. 93H § 4

§ 4. Delay in notice when notice would impede criminal investigation; cooperation with law enforcement

Effective: October 31, 2007
Currentness

Notwithstanding section 3, notice may be delayed if a law enforcement agency determines that provision of such notice may impede a criminal investigation and has notified the attorney general, in writing, thereof and informs the person or agency of such determination. If notice is delayed due to such determination and as soon as the law enforcement agency determines and informs the person or agency that notification no longer poses a risk of impeding an investigation, notice shall be provided, as soon as practicable and without unreasonable delay. The person or agency shall cooperate with law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which shall include the sharing of information relevant to the incident; provided however, that such disclosure shall not require the disclosure of confidential business information or trade secrets.

Credits
Added by St.2007, c. 82, § 16, eff. Oct. 31, 2007.

Notes of Decisions (1)

M.G.L.A. 93H § 4, MA ST 93H § 4
Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

Massachusetts General Laws Annotated
Part I. Administration of the Government (Ch. 1-182)
Title XV. Regulation of Trade (Ch. 93-110h)
Chapter 93H. Security Breaches (Refs & Annos)

M.G.L.A. 93H § 5

§ 5. Applicability of other state and federal laws

Effective: October 31, 2007
Currentness

This chapter does not relieve a person or agency from the duty to comply with requirements of any applicable general or special law or federal law regarding the protection and privacy of personal information; provided however, a person who maintains procedures for responding to a breach of security pursuant to federal laws, rules, regulations, guidance, or guidelines, is deemed to be in compliance with this chapter if the person notifies affected Massachusetts residents in accordance with the maintained or required procedures when a breach occurs; provided further that the person also notifies the attorney general and the director of the office of consumer affairs and business regulation of the breach as soon as practicable and without unreasonable delay following the breach. The notice to be provided to the attorney general and the director of the office of consumer affairs and business regulation shall consist of, but not be limited to, any steps the person or agency has taken or plans to take relating to the breach pursuant to the applicable federal law, rule, regulation, guidance or guidelines; provided further that if said person or agency does not comply with applicable federal laws, rules, regulations, guidance or guidelines, then it shall be subject to the provisions of this chapter.

Credits
Added by St.2007, c. 82, § 16, eff. Oct. 31, 2007.

M.G.L.A. 93H § 5, MA ST 93H § 5
Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

Massachusetts General Laws Annotated
Part I. Administration of the Government (Ch. 1-182)
Title XV. Regulation of Trade (Ch. 93-110h)
Chapter 93H. Security Breaches (Refs & Annos)

M.G.L.A. 93H § 6

§ 6. Enforcement of chapter

Effective: October 31, 2007
Currentness

The attorney general may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.

Credits
Added by St.2007, c. 82, § 16, eff. Oct. 31, 2007.

M.G.L.A. 93H § 6, MA ST 93H § 6
Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

EXHIBIT 2

Code of Massachusetts Regulations Currentness
Title 201: Office of Consumer Affairs and Business Regulation
Chapter 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth (Refs & Annos)

201 CMR 17.01

17.01: Purpose and Scope

(1) Purpose. 201 CMR 17.00 implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own or license personal information about a resident of the Commonwealth of Massachusetts. 201 CMR 17.00 establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of 201 CMR 17.00 is to insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

(2) Scope. 201 CMR 17.00 applies to all persons that own or license personal information about a resident of the Commonwealth.

Currency of the Update: February 13, 2015

Mass. Regs. Code tit. 201, § 17.01, 201 MA ADC 17.01

End of Document

Code of Massachusetts Regulations Currentness
Title 201: Office of Consumer Affairs and Business Regulation
Chapter 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth (Refs & Annos)

201 CMR 17.02

17.02: Definitions

The following words as used in 201 CMR 17.00 shall, unless the context requires otherwise, have the following meanings:

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 a substantial risk of identity theft or fraud against a resident of the commonwealth. 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.

Electronic, relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

Encrypted, the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Owns or Licenses, receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment.

Person, a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

Personal Information, a Massachusetts resident's first name and last name or first initial and last name in combination with any one 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; or

(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; 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.

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

Service Provider, any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person that is subject to 201 CMR 17.00.

Currency of the Update: February 13, 2015

Mass. Regs. Code tit. 201, § 17.02, 201 MA ADC 17.02

End of Document

Code of Massachusetts Regulations Currentness
Title 201: Office of Consumer Affairs and Business Regulation
Chapter 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth (Refs & Annos)

201 CMR 17.03

17.03: Duty to Protect and Standards for Protecting Personal Information

(1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to:

(a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program;

(b) the amount of resources available to such person;

(c) the amount of stored data; and

(d) the need for security and confidentiality of both consumer and employee information.

The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated.

(2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

(a) Designating one or more employees to maintain the comprehensive information security program;

(b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:

1. ongoing employee (including temporary and contract employee) training;

2. employee compliance with policies and procedures; and

3. means for detecting and preventing security system failures.

(c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises.

(d) Imposing disciplinary measures for violations of the comprehensive information security program rules.

(e) Preventing terminated employees from accessing records containing personal information.

(f) Oversee service providers, by:

1. Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with 201 CMR 17.00 and any applicable federal regulations; and

2. Requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information; provided, however, that until March 1, 2012, a contract a person has entered into with a third party service provider to perform services for said person or functions on said person's behalf satisfies the provisions of 201 CMR 17.03(2)(f)2. even if the contract does not include a requirement that the third party service provider maintain such appropriate safeguards, as long as said person entered into the contract no later than March 1, 2010.

(g) Reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers.

(h) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.

(i) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

(j) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

Currency of the Update: February 13, 2015

Mass. Regs. Code tit. 201, § 17.03, 201 MA ADC 17.03

End of Document

Code of Massachusetts Regulations Currentness
Title 201: Office of Consumer Affairs and Business Regulation
Chapter 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth (Refs & Annos)

201 CMR 17.04

17.04: Computer System Security Requirements

Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:

(1) Secure user authentication protocols including:

(a) control of user IDs and other identifiers;

(b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;

(c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;

(d) restricting access to active users and active user accounts only; and

(e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

(2) Secure access control measures that:

(a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and

(b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

(3) Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;

(5) Encryption of all personal information stored on laptops or other portable devices;

(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.

(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

Currency of the Update: February 13, 2015

Mass. Regs. Code tit. 201, § 17.04, 201 MA ADC 17.04

End of Document

201 CMR 17.05

17.05: Compliance Deadline

(1) Every person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 on or before March 1, 2010.

Currency of the Update: February 13, 2015

Mass. Regs. Code tit. 201, § 17.05, 201 MA ADC 17.05

End of Document

EXHIBIT 3

Massachusetts General Laws Annotated
Part I. Administration of the Government (Ch. 1-182)
Title XV. Regulation of Trade (Ch. 93-110h)
Chapter 93I. Dispositions and Destruction of Records (Refs & Annos)

M.G.L.A. 93I § 1

§ 1. Definitions

Effective: February 3, 2008
Currentness

As used in this chapter the following words shall, unless the context clearly requires otherwise, have the following meanings:--

“Agency”, any county, city, town, or constitutional office or any agency thereof, including but not limited to, any department, division, bureau, board, commission or committee thereof, or any authority created by the general court to serve a public purpose, having either statewide or local jurisdiction.

“Data subject”, an individual to whom personal information refers.

“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 the resident:--

(a) Social Security number;

(b) driver's license number or Massachusetts 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) a biometric indicator.

Credits
Added by St.2007, c. 82, § 17, eff. Feb. 3, 2008.

M.G.L.A. 93I § 1, MA ST 93I § 1
Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

Massachusetts General Laws Annotated
Part I. Administration of the Government (Ch. 1-182)
Title XV. Regulation of Trade (Ch. 93-110h)
Chapter 93I. Dispositions and Destruction of Records (Refs & Annos)

M.G.L.A. 93I § 2

§ 2. Standards for disposal of records containing personal information; disposal by third party; enforcement

Effective: February 3, 2008
Currentness

When disposing of records, each agency or person shall meet the following minimum standards for proper disposal of records containing personal information:

(a) paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;

(b) electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

Any agency or person disposing of personal information may contract with a third party to dispose of personal information in accordance with this chapter. Any third party hired to dispose of material containing personal information shall implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of or use of personal information during the collection, transportation and disposal of personal information.

Any agency or person who violates the provisions of this chapter shall be subject to a civil fine of not more than $100 per data subject affected, provided said fine shall not exceed $50,000 for each instance of improper disposal. The attorney general may file a civil action in the superior or district court in the name of the commonwealth to recover such penalties.

Credits
Added by St.2007, c. 82, § 17, eff. Feb. 3, 2008.

M.G.L.A. 93I § 2, MA ST 93I § 2
Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

Massachusetts General Laws Annotated
Part I. Administration of the Government (Ch. 1-182)
Title XV. Regulation of Trade (Ch. 93-110h)
Chapter 93I. Dispositions and Destruction of Records (Refs & Annos)

M.G.L.A. 93I § 3

§ 3. Enforcement

Effective: February 3, 2008
Currentness

The attorney general may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of this chapter and for other relief that may be appropriate.

Credits
Added by St.2007, c. 82, § 17, eff. Feb. 3, 2008.

M.G.L.A. 93I § 3, MA ST 93I § 3
Current through Chapters 1 to 505 of the 2014 2nd Annual Session

End of Document

EXHIBIT 4

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CIVIL ACTION NO.

COMMONWEALTH OF MASSACHUSETTS,

Plaintiff,

v.

EQUIFAX, INC.

Defendant.

COMPLAINT

JURY TRIAL REQUESTED

INTRODUCTION

1. The Commonwealth of Massachusetts, by and through its Attorney General, Maura Healey ("Commonwealth"), brings this action against Equifax, Inc. ("Equifax") pursuant to the Massachusetts Consumer Protection Act (G.L. c. 93A) and the Massachusetts Data Security Law (G.L. c. 93H).

2. Equifax is one of three primary national credit-reporting bureaus in the United States. Equifax collects and maintains data regarding more than 820 million consumers worldwide, including at least 3,000,000 in Massachusetts. The personal data that Equifax holds touches upon virtually every aspect of a consumer's profile in the marketplace.

3. Equifax is a gatekeeper for consumers' access to socioeconomic opportunity and advancement. Every day, businesses across the country rely on Equifax's credit profiles to make decisions as to the credit worthiness of consumers. This information impacts many of the most important decisions in the lives of consumers—for instance, whether consumers can buy a house, obtain a loan, lease a vehicle, or even get a job.

4. Consumers do not choose to give their private information to Equifax, and they do not have any reasonable manner of preventing Equifax from collecting, processing, using, or disclosing it. Equifax largely controls how, when, and to whom the consumer data it stockpiles is disclosed. Likewise, consumers have no choice but to rely on Equifax to protect their most sensitive and personal data. Accordingly, it was and is incumbent on Equifax to implement and maintain the strongest safeguards to protect this data. Equifax has failed to do so.

5. From at least March 7, 2017 through July 30, 2017, a period of almost five months, Equifax left at least 143 million consumers' sensitive and private information exposed and vulnerable to intruders by relying on certain open-source code (called "Apache Struts") that it knew or should have known was insecure and subject to exploitation. Although patches, workarounds, and other fixes for the vulnerability were available and known to Equifax as of March 7, 2017, Equifax failed to avail itself of these remedies or employ other compensating security controls, such as encryption or multiple layers of security, that were sufficient to protect consumers' personal data.

6. As a result, intruders were able to access Equifax's computer system from at least May 13, 2017 through July 30, 2017, and potentially stole the sensitive and personal information of 143 million consumers (the "Data Breach"). The Data Breach, which Equifax first disclosed to the public on September 7, 2017, exposed to still-unknown persons some of the most sensitive and personal data of Massachusetts residents, including full names, social security numbers, dates of birth, addresses, and for some consumers, credit card numbers, driver's license numbers, and/or other unknown, personally-identifiable information.

7. Equifax could have—and should have—prevented the Data Breach had it implemented and maintained reasonable safeguards, consistent with representations made to the

public in its privacy policies, industry standards, and the requirements of Massachusetts law. Equifax did not do so.

8. By failing to secure consumer information, Equifax exposed over half of the adult population of Massachusetts to the risks of identity theft, tax return scams, financial fraud, health identity fraud, and other harm. Affected consumers have spent, and will continue to spend, money, time, and other resources attempting to protect against an increased risk of identity theft or fraud, including by placing security freezes over their credit files and monitoring their credit reports, financial accounts, health records, government benefit accounts, and any other account tied to or accessible with a social security number. The increased risk of identity theft and fraud as a result of the Data Breach also has caused Massachusetts consumers substantial fear and anxiety and likely will do so for many years to come.

9. Given the nature of Equifax's business, the sensitivity and volume of the data in which it traffics, and the serious consequences to consumers when that data is exposed, its failure to secure this information constitutes a shocking betrayal of public trust and an egregious violation of Massachusetts consumer protection and data privacy laws. As Equifax's own Chairman and Chief Executive Officer admitted, the Data Breach "strikes at the heart of who we are and what we do."

10. By this action the Commonwealth seeks to ensure that Equifax is held accountable, and not allowed to prioritize profits over the safety and privacy of consumers' sensitive and personal data. The Commonwealth seeks civil penalties, disgorgement of profits, restitution, costs, and attorney's fees, as available under G.L. c. 93A and G.L. c. 93H. The Commonwealth also seeks all necessary, appropriate, and available equitable and injunctive

relief to address, remedy, and prevent harm to Massachusetts residents resulting from Equifax's actions and inactions.

THE PARTIES

11. The Plaintiff is the Commonwealth of Massachusetts, represented by its Attorney General, who brings this action in the public interest pursuant to G.L. c. 93A, § 4, and G.L. c. 93H, § 6.

12. Defendant Equifax, Inc. is a publicly-traded Georgia corporation with its principal place of business at 1550 Peachtree Street N.E., Atlanta, Georgia.

JURISDICTION, AUTHORITY, AND VENUE

13. The Attorney General is authorized to bring this action, in this Court, under G.L. c. 93A, § 4, and G.L. c. 93H, § 6.

14. This Court has jurisdiction over the subject matter of this action by virtue of G.L. c. 93A, § 4, and G.L. c. 212, § 4.

15. This Court has personal jurisdiction over Equifax under G.L. c. 223A, § 3, including because Equifax has engaged in business with Massachusetts entities, and because Equifax's actions and inactions have affected Massachusetts residents.

16. Venue is proper in Suffolk County under G.L. c. 93A, § 4, as Equifax "has no place of business within the commonwealth," and under G.L. c. 223, § 5, as the Commonwealth is the plaintiff.

17. The Commonwealth notified Equifax of its intent to bring this action at least five days prior to the commencement of this action, as required by G.L. c. 93A, § 4.

FACTS

Equifax's Business

18. Equifax's business centers on the collection, processing, and sale of information about people and businesses. According to its website, Equifax is a "global information solutions company" that "organizes, assimilates, and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers." Equifax employs approximately 9,900 people worldwide.

19. As part of its business, Equifax creates, maintains, and sells "credit reports" and "credit scores" regarding individual consumers, including Massachusetts residents. Credit reports can contain, among other things, an individual's full social security number, current and prior addresses, age, employment history, detailed balance and repayment information for financial accounts, bankruptcies, judgments, liens, and other sensitive information. The credit score is a proprietary number, derived from a credit report and other information, that is intended to indicate relative to other persons whether a person would be likely to repay debts.

20. Third parties use credit reports and credit scores to make highly consequential decisions affecting Massachusetts consumers. For instance, credit scores and/or credit reports are used to determine whether an individual qualifies for a mortgage, car loan, student loan, credit card, or other form of consumer credit; whether a consumer qualifies for a certain bank account, insurance, cellular phone service, or cable or internet service; the individual's interest rate for the credit they are offered; the amount of insurance premiums; whether an individual can rent an apartment; and even whether an individual is offered a job.

The Data Breach

21. At all relevant times, Equifax maintained a publicly available website at www.equifax.com.

22. Within that website are various publicly available web pages directed to consumers, including Massachusetts residents. Among those web pages is one through which Equifax invites consumers to submit information to initiate and support a formal dispute of information in their credit reports (the "Dispute Portal").

23. Equifax maintained consumer names, addresses, full social security numbers, dates of birth, and for some consumers, driver's license numbers and/or credit card numbers of at least 143 million consumers, including nearly 3 million Massachusetts residents, in computer tables, databases, or files that were accessible (directly or indirectly) through the Dispute Portal (the "Exposed Information"). The Exposed Information, which included "Personal Information" as defined in G.L. c. 93H, § 1, and 201 CMR. 17.02, was not limited to the sensitive and personal information of those consumers who had used the Dispute Portal, but encompassed a larger group of consumers on whom Equifax held information.

24. Despite being accessible through a publicly available website, the Exposed Information was not "encrypted" on Equifax's systems as defined in 201 CMR 17.02.

25. Starting on or about May 13, 2017 through July 30, 2017, unauthorized third parties infiltrated Equifax's computer system via the Dispute Portal. Once in, the parties accessed and likely stole (i.e. "exfiltrated") the Exposed Information from Equifax's network.

Equifax Ignored Numerous Signs that Its System —and the Consumers' Data Stored Therein—Was Vulnerable to Hackers

26. According to a statement Equifax published online at https://www.equifaxsecurity2017.com on or about September 13, 2017, the Data Breach resulted when "criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638."

27. Apache Struts is a piece of computer code used for creating web applications; i.e. a computer program that runs in a web browser.

28. At all relevant times, Equifax used Apache Struts, in whole or in part, to create, support, and/or operate its Dispute Portal.

29. As "open-source code," Apache Struts is free and available for anyone to download, install, or integrate into their computer system. Apache Struts, like many other pieces of open-source code, comes with no warrantees of any kind, including warrantees about its security. Accordingly, it is incumbent on companies that use Apache Struts—like Equifax—to assess whether the open-source code is appropriate and sufficiently secure for the company's purposes and that it is kept up-to-date and secure against known vulnerabilities.

30. There are, and at all relevant times have been, multiple well-known resources available to support companies relying on open-source code, including Apache Struts. These resources publicly announce to users when security vulnerabilities in the open-source code are discovered and verified, including in Apache Struts, compare the associated risks of such vulnerabilities, and propose fixes.

31. For example, the Apache Software Foundation ("Apache"), a non-profit corporation, releases updated versions of Apache Struts to "patch" it against verified security vulnerabilities. Apache also releases Security Bulletins on its website regarding security flaws in

Apache Struts, noting the nature of the vulnerability and ways to resolve it. Since 2007, Apache has posted at least 53 such security bulletins for Apache Struts.

32. Similarly, the U.S. Department of Commerce's National Institute of Standards and Technology ("NIST") maintains a free and publicly available National Vulnerability Database ("NVD") at http://nvd.nist.gov. Using the NVD, NIST identifies security vulnerabilities, including in open-source code, the risks they pose, and ways to fix them, including as to security vulnerabilities in Apache Struts.

33. Likewise, the MITRE Corporation, a "not-for-profit organization that operates research and development centers sponsored by the [United States] federal government,"[1] also identifies code security vulnerabilities, including vulnerabilities in Apache Struts, using a Common Vulnerabilities and Exposures ("CVE") Identifier. According to MITRE, the CVE Identifier is the industry standard for identifying publicly known cyber security vulnerabilities. MITRE maintains a database of CVE identifiers and the vulnerabilities to which they correspond, which is publicly accessible without cost online at https://cve.mitre.org (the "Vulnerability Database").

34. On March 7, 2017, Apache published notice of a security vulnerability in certain versions of Apache Struts in its online security bulletins S2-045 and S2-046 (the "Apache Security Bulletins"). **Exhibit 1** (https://cwiki.apache.org/confluence/display/WW/S2-045 last visited September 19, 2017) and **Exhibit 2** (https://cwiki.apache.org/confluence/display/WW/S2-046 last visited September 19, 2017). The vulnerability was assigned the CVE identifier CVE-2017-5638 (the "March Security Vulnerability").

[1] https://www.mitre.org/.

35. Directed to "All Struts2 developers and users," the Apache Security Bulletins warned that the software was vulnerable to "Remote Code Execution," or "RCE." RCE refers to a method of hacking a public website whereby an online attacker can send computer code to the website that allows the attacker to infiltrate (that is, gain access to), and run commands on the website's server (the computer that stores the information that supports the website).

36. The Apache Security Bulletins assigned the March Security Vulnerability a "maximum security rating" of "critical." Apache recommended that users update the affected versions of Apache Struts to fix the vulnerability, or to implement other specific workarounds to avoid the vulnerability. **Exhibits 1 and 2.**

37. NIST also publicized the March Security Vulnerability in its NVD on or about March 10, 2017. **Exhibit 3** (https://nvd.nist.gov/vuln/detail/CVE-2017-5638, last visited September 19, 2017) (the "NIST Notice"). NIST noted that the severity of the vulnerability was an overall score of 10.0 on two different versions of a scale called the Common Vulnerability Scoring System ("CVSS"). A score of 10.0 is the highest possible severity score on either scale. The NIST Notice also stated that an attack based on the vulnerability "[a]llows unauthorized disclosure of information," would be low in complexity to accomplish, and would not require the attacker to provide authentication (for example, a user name and password) to exploit the vulnerability. The NIST Notice also documented over twenty other website resources for advisories, solutions, and tools related to the March Security Vulnerability and how to patch or fix it.

38. Following the NIST Notice, the United States Computer Emergency Readiness Team ("US CERT") issued a security Bulletin (Bulletin (SB17-079)) on March 20, 2017, calling out the March Security Vulnerability as a "High" severity vulnerability ("US CERT Alert").

Exhibit 4 (excerpts from https://www.us-cert.gov/ncas/bulletins/SB17-079, last visited September 19, 2017) (relevant entry highlighted).

39. Likewise, MITRE included the March Security Vulnerability in the Vulnerability Database and documented various external website references to the March Security Vulnerability. **Exhibit 5 (**https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638, last visited September 19, 2017).

40. In the days following the public disclosure of the March Security Vulnerability by Apache, media reports claimed that hackers were exploiting the March Security Vulnerability against numerous companies, including banks, government agencies, internet companies, and other websites.

41. As Equifax disclosed on its website on or about September 13, 2017, the Data Breach occurred as a result of the exploitation of the March Security Vulnerability by hackers.

42. As of or soon after March 7, 2017, Equifax knew or should have known, by virtue of multiple public sources but at least one or all of the Apache Security Bulletins, the NIST Notice, the US CERT Alert, and the Vulnerability Database (as well as one or all of the various collateral sources referenced in the foregoing), that the March Security Vulnerability existed in Apache Struts.

43. Indeed, in a notice on the website https://www.equifaxsecurity2017.com/, Equifax stated that "Equifax's Security organization was aware of this vulnerability" in Apache Struts in early March 2017.

44. As of or soon after March 7, 2017, Equifax knew or should have known, by virtue of multiple public sources but at least one or all of the Apache Security Bulletins, the NIST Notice, the US CERT Alert, and the Vulnerability Database (as well as one or all of the various

collateral sources referenced in the foregoing), that the implementation of Apache Struts it employed on its websites, including without limitation, the Dispute Portal was susceptible to the March Security Vulnerability.

45. As of or soon after March 7, 2017, Equifax knew or should have known, by virtue of multiple public sources but at least one or all of the Apache Security Bulletins, the NIST Notice, the US CERT Alert, and the Vulnerability Database (as well as one or all of the various collateral sources referenced in the foregoing), that it was vulnerable to unauthorized access to sensitive and personal consumer information by exploitation of the March Security Vulnerability by hackers.

46. Until at least July 30, 2017, and during the Data Breach, Equifax continued to use an Apache Struts-based web application that was susceptible to the March Security Vulnerability for its Dispute Portal.

47. Until at least July 30, 2017, and during the Data Breach, Equifax failed to employ successfully recommended fixes or workarounds, otherwise patch or harden its systems, or put in place any compensating controls sufficient to avoid the March Security Vulnerability, safeguard the Exposed Information, or prevent the Data Breach.

48. In addition, until at least July 29, 2017, and during the Data Breach, Equifax did not detect and/or appropriately respond to evidence that unauthorized parties were infiltrating its computer systems and had access to the Exposed Information; and/or did not detect or appropriately respond to evidence that those parties were exfiltrating the Exposed Information out of Equifax's computer system.

49. As a result of Equifax's actions and inactions, the Data Breach occurred, and hackers were able to access and likely stole the sensitive and personal data of 143 million consumers, including of Massachusetts consumers.

Equifax's Security Program Fell Short of Its Promises to Consumers and Massachusetts Law

50. At all relevant times, Equifax promised the public that safeguarding consumers' sensitive, personal information is "a top priority."

51. At all relevant times on its Privacy Policy, available through a hyperlink at the bottom of each page of its public website, Equifax represented to the public:

> We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax.

52. Equifax likewise represented to consumers that it would keep all of their credit information, including that which consumers submitted through the Dispute Portal, secure. In its "Consumer Privacy Policy for Personal Credit Reports," accessible at http://www.equifax.com/privacy/personal-credit-reports, Equifax represented that it has "reasonable, physical, technical and procedural safeguards to help protect your [i.e. consumers'] personal information."

53. By failing to patch or otherwise address the March Security Vulnerability, detect the hackers in their network, prevent them from accessing and stealing the Exposed Information, and otherwise failing to safeguard the Exposed Information, as set forth in paragraphs 21 to 49 herein, Equifax failed to live up to its representations to the public.

54. Equifax also failed to comply with Massachusetts Law.

55. The Massachusetts Data Security Regulations, promulgated pursuant to G.L. c. 93H, § 2(a), went into effect on March 1, 2010. The objectives of the Data Security Regulations are to "insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer." G.L. c. 93H, § 2(a).

56. The Data Security Regulations "establish minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records." 201 CMR 17.01(1). These minimum standards include, among others, the development, implementation, and maintenance of a comprehensive written information security program (a "WISP") that contains enumerated, minimum safeguards to secure personal information owned or licensed by the entity. See 201 CMR 17.03.

57. The Data Security Regulations also require that an entity "establish[] and maint[ain] . . . a security system covering its computers" that contains certain minimum enumerated safeguards to prevent security compromises. See 201 CMR 17.04.

58. By failing to patch or otherwise sufficiently address the March Security Vulnerability, detect and appropriately respond to the presence of unauthorized parties in its network, prevent those parties from accessing and/or stealing the Exposed Information, and/or safeguard the Exposed Information, as set forth in paragraphs 21 to 49 herein, Equifax failed to develop, implement, or maintain a WISP that met the minimum requirements of the Data Security Regulations, 201 CMR 17.03 and 17.04.

59. In addition, the Data Security Regulations required Equifax to go beyond these minimum requirements and develop, implement, or maintain in its WISP additional safeguards that were "appropriate to" the "size, scope and type of business" of Equifax, the "amount of resources available to [it]," the "amount of stored data," and "the need for security and confidentiality of both consumer and employee information." 201 CMR 17.03(1).

60. Equifax is a large, sophisticated, multinational company of nearly 10,000 employees and billions of dollars in annual revenue whose primary business consists of acquiring, compiling, analyzing, and selling sensitive and personal data. Equifax holds the personal information and other personal data of more than 820 million consumers internationally—more than twice the population of the United States. This includes information that is sought after by hackers because it can be used to commit identity theft and financial fraud. As such, the Data Security Regulations required Equifax to implement administrative, technical, and physical safeguards that substantially exceed the minimum standards set forth in the Data Security Regulations, and which are at least consistent with industry best practices.

61. For example, and without limitation, Equifax's size, scope and type of business, the amount of resources available to it, the amount of stored data, and the need for security and confidentiality of both consumer and employee information made it "appropriate" and necessary under the Data Security Rules for Equifax to have encrypted any Personal Information that was accessible via the publicly accessible, and vulnerable, Dispute Portal. It was also "appropriate" and necessary for Equifax to have maintained multiple layers of security sufficient to protect personal information stored in its system should other safeguards fail. By failing to do so, Equifax failed to comply with 201 CMR 17.03(1).

Equifax Delayed Notifying the Public of the Data Breach

62. Chapter 93H requires covered entities to report data breaches to the Commonwealth, including the Attorney General's Office and the Office of Consumer Affairs and Business Regulation, "as soon as practicable and without unreasonable delay, when such person . . . (1) knows or has reason to know of a breach of security [as that term is defined in G.L. c. 93H, § 1(a)], or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose[.]" G.L. c. 93H, § 3(b).

63. As of or soon after July 29, 2017, Equifax knew or should have known that the "personal information" (as defined in G.L. c. 93H, § 1(a)) of at least one Massachusetts resident was acquired by an unauthorized person, and/or of a "breach of security," and that it thus had a duty to provide notice to the Attorney General's Office and the Office of Consumer Affairs and Business Regulation under chapter 93H, § 3(b) "as soon as reasonably practicable and without unreasonable delay."

64. Equifax delayed providing notice to the Attorney General or the Office of Consumer Affairs and Business Regulation until September 7, 2017. Equifax thus failed to provide timely notice under chapter 93H, § 3(b).

65. Chapter 93H, § 3(b) also requires an entity to provide timely written notice, with content specified by § 3(b), of a reportable data breach to each affected consumer. Such notice, when promptly given, allows the consumer to take steps to protect him or herself from identity theft, fraud, or other harm that may result from the breach.

66. Under chapter 93H, § 1, a breached entity may provide "substitute notice" to consumers "if the person . . . 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 . . . does not have sufficient contact information to provide notice." Substitute notice consists of all three of the following: (1) email notice to the extent the entity has email addresses for the affected residents, (2) a "clear and conspicuous posting of the notice on the home page" of the notifying entity and (3) "publication in or broadcast through media or medium that provides notice throughout the commonwealth." G.L. c. 93H, §1.

67. Equifax knew or should have known as of or soon after July 29, 2017, that it met the threshold for being able to provide "substitute notice" as defined in chapter 93H, § 1.

68. Despite this, Equifax did not then avail itself of any element of the substitute notice process but instead delayed notifying the public of the Data Breach for nearly six weeks, until September 7, 2017, through a website posting. Equifax thus failed to provide timely notice to affected consumers as required by chapter 93H, § 3(b).

Equifax's Actions and Inactions in Connection with the Data Breach Have Created, Compounded, and Exacerbated the Harms Suffered by the Public

69. The Attorney General is not required to demonstrate harm to consumers in order to enforce the Data Breach Notice Law (G.L. c. 93H), the Data Security Regulations (201 CMR 17.00–17.05), or the Consumer Protection Act (G.L. c. 93A).

70. Nevertheless, consumers clearly have already suffered significant and lasting harm as a result of the Data Breach, and such harm is likely to continue and worsen over time.

71. Armed with an individual's sensitive and personal information—including in particular a social security number, date of birth, and/or a drivers' license number—a criminal can commit identity theft, financial fraud, and other identity-related crimes. According to the Federal Trade Commission ("FTC"):

> Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.[2]

72. Identity theft results in real financial losses, lost time, and aggravation to consumers. In its 2014 Victims of Identity Theft report, the United States Department of Justice stated that 65% of the over 17 million identity theft victims that year suffered a financial loss, and 13% of the total identity theft victims never had those losses reimbursed.[3] The average out-of-pocket loss for those victims was $2,895. Identity theft victims also "paid higher interest rates on credit cards, they were turned down for loans or other credit, their utilities were turned off, or they were the subject of criminal proceedings."[4] With respect to consumers' emotional distress, the report also noted that more than one-third of identity theft victims were moderately or severely distressed due to the crime.[5]

73. The Data Breach has substantially increased the risk that the affected Massachusetts consumers will be a victim of identity theft or financial fraud at some unknown point in the future.

---

[2] See https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft.

[3] U.S. Dept. of Justice, Bureau of Justice Statistics, Victims of Identity Theft 2014, at 6 & Table 6, *available at* http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408.

[4] Id. at 8.

[5] See id. at 9, Table 9.

74. In order to protect themselves from this increased risk of identity theft and fraud, many consumers may place "security freezes" on their credit reports with one or more consumer reporting agency, including Equifax. The primary objective of a security freeze is to prevent third parties from accessing the frozen credit report when a new application for credit is placed without the consumer's consent.

75. Massachusetts law permits, but does not require, the consumer reporting agency to charge the consumer a "reasonable fee, not to exceed $5," to place, lift, or remove a freeze on the consumer's credit report. See G.L. c. 93, § 62A.

76. As a result of Equifax's actions and inactions in connection with the Data Breach, and in an effort to protect themselves against identity theft or financial fraud, many Massachusetts consumers have already spent and will continue to spend time and money in an effort to place security freezes on their credit reports with Equifax and other consumer reporting agencies.

77. Further, Equifax has complicated consumers' efforts to protect themselves from the harms caused by the Data Breach by failing to take various measures that it was uniquely positioned to take to mitigate the risk of harm caused by the Data Breach. Instead, Equifax has failed to clearly and promptly notify consumers whether they were affected by the Data Breach, has charged consumers to place security freezes (and presumably unfairly profited thereby), has failed to offer consumers free credit and fraud monitoring beyond one year, and has failed to ensure adequate call center staffing and availability of online services in the days following the September 7, 2017 announcement of the Data Breach. Equifax's actions and inactions in this regard have compounded the harms already suffered by consumers.

CAUSES OF ACTION

COUNT I

Violations of G.L. c. 93H, § 3 – Failure to Give Prompt Notice of Data Breach

78. The Commonwealth incorporates and realleges herein the allegations in paragraphs 1–77.

79. The Commonwealth "may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of [c. 93H] and for other relief that may be appropriate." G.L. c. 93H, § 6.

80. As a corporation, Equifax is a "person" under G.L. c. 93H, § 1(a).

81. General Laws c. 93H, § 3(b) requires that a person who:

> [O]wns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the attorney general, the director of consumer affairs and business regulation and to such resident in accordance with this chapter.

82. "Personal Information" is defined in G.L. c. 93H, § 1(a) as:

> [A] [Massachusetts] 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; or (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 . . . .

83. At all relevant times, Equifax owned or licensed personal information of at least one Massachusetts resident, as the term "personal information" is defined in G.L. c. 93H, § 1(a).

84. As of or soon after July 29, 2017, Equifax knew or should have known that the "personal information" (as defined in G.L. c. 93H, § 1(a)) of at least one Massachusetts resident

was acquired by an unauthorized person, and/or that the Data Breach was a "breach of security" as defined in G.L. c. 93H, § 1(a).

85. As of or soon after July 29, 2017, Equifax knew or should have known that it met the threshold for being able to provide "substitute notice" to Massachusetts residents as defined in G.L. 93H, § 1(a).

86. Equifax did not provide notice to the Attorney General, the Office of Consumer Affairs and Business Regulation, and affected consumers until September 7, 2017.

87. By not providing notice, substitute or otherwise, "as soon as practicable and without unreasonable delay" to the Attorney General, the Office of Consumer Affairs and Business Regulation, and affected consumers, Equifax violated G.L. c. 93H, § 3(b).

88. Each failure to notify each affected Massachusetts consumer, the Attorney General, and the Office of Consumer Affairs and Business Regulation constitutes a separate violation of G.L. c. 93H.

COUNT II

Violations of G.L. c. 93H/201 CMR 17.00–17.05 – Failure to Safeguard Personal Information

89. The Commonwealth hereby incorporates and realleges the allegations in paragraphs 1–88.

90. The Commonwealth "may bring an action pursuant to section 4 of chapter 93A against a person or otherwise to remedy violations of [c. 93H] and for other relief that may be appropriate." G.L. c. 93H, § 6.

91. The Data Security Regulations, 201 CMR 17.00-17.05, were promulgated under authority of G.L. c. 93H, § 2.

92. The Data Security Regulations "apply to all persons that own or license personal information about a resident of the Commonwealth." 201 CMR 17.01(2).

93. As a corporation, Equifax is a "person" under the Data Security Regulations. See 201 CMR 17.02.

94. The definition of "Personal Information" in the Data Security Regulations is coextensive to the definition of "Personal Information" in G.L. c. 93H, § 1, which is set forth in paragraph 82. See 201 CMR 17.02.

95. An entity "owns or licenses" personal information under the Data Security Regulations if it "receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment." 201 CMR 17.02.

96. Equifax is bound by the Data Security Regulations because at all relevant times, it owned or licensed personal information of at least one Massachusetts resident and continues to own or license the personal information of Massachusetts residents.

97. The Data Security Regulations "establish[] minimum standards to be met in the connection with the safeguarding of personal information contained in both paper and electronic records." 201 CMR 17.01(1).

98. Among these minimum standards is the duty of "[e]very person that owns or licenses personal information about a resident of the Commonwealth" to "develop, implement, and maintain" a written information security program (a "WISP") that "contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope and type of business . . . ; (b) the amount of resources available to such person; (c) the amount of stored data; and

(d) the need for security and confidentiality of both consumer and employee information." 201 CMR 17.03(1).

99. The Data Security Regulations mandate certain minimum safeguards and obligations that an entity must develop, implement, and maintain in its WISP, including among others:

- To "[i]dentify[] and assess[] reasonably foreseeable internal and external risks to the security,confidentiality, and/or integrity of any electronic . . . records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks[.]" (201 CMR 17.03(2)(b));

- "[M]eans for detecting and preventing security system failures." (201 CMR 17.03(2)(b)(3)); and

- "Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks." (201 CMR 17.03(2)(h)).

100. The WISP must also include the "the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible," contains certain minimum elements, including:

- "Secure user authentication protocols including . . . (a) control of user IDs and other identifiers; (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect; (d) restricting access to active users and active user accounts only; and (e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system[.] (201 CMR 17.04(1));

- "[S]ecure access control measures" over computer systems that "restrict access to records and files containing personal information to those who need such information to perform their job duties . . . ." (201 CMR 17.04(2)(a));

- "[S]ecure access control measures" over computer systems that "(b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls[.]" (201 CMR 17.04(2)(b));

- "Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly." (201 CMR 17.04(3));

- "Reasonable monitoring of systems, for unauthorized use of or access to personal information[.]" (201 CMR 17.04(4));

- "For files containing personal information on a system that is connected to the Internet, . . . reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information[.]" (201 CMR 17.04(6)); and

- "Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis." (201 CMR 17.04(7)).

101. Equifax failed to develop, implement, and maintain its WISP and a security system covering its computers in such a way as to meet the minimum requirements of 201 CMR 17.03 and 201 CMR 17.04, including without limitation the minimum requirements set forth in 201 CMR 17.03(2)(b), (2)(b)(3), or (2)(h)); or 201 CMR 17.04(1), (2)(a), (2)(b), (3), (4), (6), or (7).

102. Equifax also failed to satisfy its obligations to develop, implement, and maintain a WISP that contained "administrative, technical, and physical safeguards that are appropriate" to: (a) "the size, scope and type of business of" Equifax; (b) "the amount of resources available to" Equifax; (c) the amount of data Equifax stores; and (d) "the need for security and confidentiality of both consumer and employee information." 201 CMR 17.03(1).

103. These failures include, without limitation: not adequately patching or implementing other safeguards sufficient to avoid the March Security Vulnerability; keeping the Exposed Information unencrypted or otherwise not protected through other methods from unauthorized disclosure in an area of its network accessible to the Internet; and not maintaining multiple layers of security sufficient to protect personal information from compromise.

104. Each violation of the Data Security Regulations as to each affected Massachusetts resident is a separate violation of c. 93H, § 2.

105. Accordingly, Equifax violated G.L. c. 93H, § 2.

COUNT III

Violations of G.L. c. 93A, § 2 – Unfair Acts or Practices

106. The Commonwealth hereby incorporates and realleges the allegations in paragraphs 1–105.

107. General Laws c. 93A, § 2(a) declares unlawful " unfair or deceptive acts or practices in the conduct of trade or commerce[.]"

108. Equifax conducts trade and commerce in Massachusetts and with Massachusetts consumers.

109. As a corporation, Equifax is a "person" under G.L. c. 93A, § 1(a).

110. Equifax has engaged in unfair or deceptive acts or practices in violation of G.L. c. 93A § 2(a).

111. Equifax's unfair or deceptive acts or practices include: (a) failing to promptly notify the public (including the Attorney General's Office and affected residents) of the Data Breach despite the existence of substantial risk to consumers from the Data Breach; and/or (b) failing to maintain reasonable safeguards sufficient to secure the private and sensitive information about Massachusetts consumers from known and foreseeable threats of unauthorized access or unauthorized use, including identity theft, financial fraud, or other harms.

112. In addition, each of Equifax's violations of G.L. c. 93H and 201 CMR 17.00–17.05, as alleged herein and in Counts I & II, *supra*, are unfair or deceptive acts or practices in violation of G.L. c. 93A, § 2(a).

113. Accordingly, Equifax violated G.L. c. 93A, § 2.

114. Each and every violation of G.L. c. 93H and 201 CMR 17.00–17.05 with respect to each Massachusetts consumer is a separate violation of G.L. c. 93A, § 2.

115. Equifax knew or should have known that each of its violations of G.L. c. 93H and 201 CMR 17.00–17.05, each failure to maintain reasonable safeguards to protect Massachusetts consumers' sensitive and personal information, and each failure to promptly notify the public of the Data Breach, would violate G.L. c. 93A, § 2.

116. Although consumer harm is not an element of a claim under c. 93A, § 4, each and every consumer affected by the Data Breach has suffered and/or will suffer financial losses, and the associated stress and anxiety, as a result of the above unfair or deceptive acts or practices, including without limitation the costs to place, lift, and/or terminate security freezes with all applicable consumer reporting bureaus, remedial measures to prevent or respond to identity theft or other fraud, and out of pocket losses resulting therefrom.

COUNT IV

Violation of G.L. c. 93A, § 2 – Deceptive Acts or Practices

117. The Commonwealth hereby incorporates and realleges the allegations in paragraphs 1–116.

118. At all relevant times, Equifax represented to the public on its online Privacy

Policy that it has:

> [B]uilt our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax.

119. In its "Consumer Privacy Policy for Personal Credit Reports," accessible at http://www.equifax.com/privacy/personal-credit-reports, Equifax further publicly represented that it has "reasonable, physical, technical and procedural safeguards to help protect your [i.e. consumers'] personal information."

120. Equifax's failures: to patch or otherwise adequately address the March Security Vulnerability; detect the hackers in their network; prevent them from accessing and stealing the Exposed Information; and otherwise failing to safeguard the Exposed Information, as alleged in paragraphs 21 to 49, herein, rendered these representations deceptive.

121. Additionally, Equifax's failure to implement, develop, and/or maintain a WISP compliant with the Data Security Regulations or industry standards, as alleged in paragraphs 50 to 61 and 89 to 105, herein, rendered these representations deceptive.

122. Equifax's public representations of the nature of its security safeguards over Massachusetts consumers' sensitive and personal information were unfair or deceptive under G.L. c. 93A, § 2(a).

123. Accordingly, Equifax violated G.L. c. 93A, § 2.

124. Equifax knew or should have known that its misrepresentations of the nature of its security safeguards over Massachusetts consumers' sensitive and personal information would violate G.L. c. 93A, § 2.

COUNT V

Violation of G.L. c. 93A , § 2 – Unfair or Deceptive Trade Practices

125. The Commonwealth hereby incorporates and realleges the allegations in paragraphs 1– 124.

126. Equifax committed unfair or deceptive acts or practices under G.L. c. 93A, § 2, by failing to adequately allow or otherwise hindering the ability of Massachusetts consumers to protect themselves from harm resulting from the Data Breach by failing to make sufficiently available measures that Equifax was uniquely positioned to provide to mitigate the public harm caused by the Data Breach, namely:

- Timely notice of the Data Breach;
- Free security freezes of Equifax credit reports;
- Free Credit and fraud monitoring of Equifax credit reports for more than one year;
- Ensuring adequate and competent call center staffing related to the Data Breach; and
- Ensuring the availability of online services that notified consumers of whether they were affected by the Data Breach and allowed consumers to place a security freeze.

127. Accordingly, Equifax violated G.L. c. 93A, § 2.

128. Equifax knew or should have known that that the conduct described in paragraphs 69 to 77and 125 to 126 would violate G.L. c. 93A, § 2.

PRAYER FOR RELIEF

WHEREFORE, the Commonwealth requests that the Court grant the following relief:

1. Enter a permanent injunction prescribing appropriate relief;

2. Order that Equifax pay civil penalties, restitution, and costs of investigation and litigation of this matter, including reasonable attorney's fees, to the Commonwealth of Massachusetts as provided for under G.L c. 93A, § 4, in an amount to be determined at trial;

3. Disgorge profits Equifax obtained during or as a result of the Data Breach; and

4. Order such other just and proper legal and equitable relief.

REQUEST FOR JURY TRIAL

The Commonwealth hereby requests trial by jury as to all issues so triable.

Respectfully submitted,

COMMONWEALTH OF MASSACHUSETTS

MAURA HEALEY
ATTORNEY GENERAL

By: _____

Sara Cable (BBO #667084)
Jared Rinehimer (BBO #684701)
Michael Lecaroz (BBO #672397)
Assistant Attorneys General
Consumer Protection Division
One Ashburton Place, 18th Floor
Boston, MA 02108
(617) 727-2200
sara.cable@state.ma.us
jared.rinehimer@state.ma.us
michael.lecaroz@state.ma.us

Date: September 19, 2017