



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 Financial Services Committee

Continuation of Hearing Entitled “Examining the Equifax Data Breach”

October 25, 2017

I. Introduction

Chairman Hensarling, Ranking Member Waters, and members of the Committee, thank you for inviting me to testify today regarding the recent Equifax breach. 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 September 19, our Office filed the first state enforcement suit against Equifax. Our goal is to hold the company accountable for the harms the breach has caused nearly 3 million Massachusetts consumers – half of our adult population.¹

We sued Equifax because, in our view, the company left hundreds of millions of records consisting of consumers’ most sensitive personal information 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 Law, and that it compounded consumers’ harm by charging consumers to implement security freezes necessitated by its own mistakes. Our view is that Equifax could have and should have prevented this breach.

The implications of the Equifax breach go far beyond the failure of one company to secure consumer data. While the Equifax breach may be unique in its scope, the failure to reasonably secure consumers’ data from foreseeable threats is an ongoing challenge for organizations in every sector. The Equifax breach also raises broader questions about the collection, sale, and use of consumer data in the consumer reporting industry. I want to highlight three key points.

¹ A copy of our Complaint is attached as **Exhibit 1**.

First, it appears to us that organizations that profit off consumers' data are not taking reasonable steps to secure it from foreseeable threats of compromise. Over the last ten years, our Office has received notice of over 19,000 data breaches impacting millions of Massachusetts residents. The failure by a business to take seriously the security of the consumer data while profiting off that data it is unfair and undermines the consumer trust necessary for a thriving information-based economy. Stronger laws coupled with more aggressive enforcement are needed to ensure that organizations are incentivized to protect consumers' data from unauthorized use or access.

Second, consumers lack adequate protections and recourse when their data is compromised – an increasing probability for nearly every US consumer. Consumers currently have to jump through too many hoops and pay too much money to freeze their credit files – one of the best ways to protect themselves after a data breach. Consumers likewise face too many challenges in obtaining compensation for losses caused by an entity's failure to protect their data. Consumers must be able to easily and quickly freeze their credit files for free, without giving up any legal rights or having to further share personal information. Consumers also should be able to seek legal redress and compensation – in addition to any other monetary losses they may suffer – for the time and money spent responding to a breach. Because ascertaining actual damages may be difficult, consumers should be entitled to seek (the higher of) actual damages, or meaningful statutory damages when their information is compromised by a business's failure to reasonably secure it.

Third, consumers lack meaningful control over who gets their data, the circumstances under which their data is taken, and what is being done with their data. According to Equifax, the breached data did not come from its core consumer or commercial credit reporting databases, but was a separate cache stored elsewhere. It is not yet clear how Equifax obtained this data or what it was used for. Many consumers did not knowingly choose to give this data to Equifax and did not knowingly choose to do business with them, yet now have to suffer the consequences of Equifax's mistakes. Consumers must have more control over who is collecting their personal data and how it is being used so that they can assess the risks of sharing it.

II. Companies Continue to Struggle to Safeguard Consumer Data from Foreseeable and Preventable Risks.

A. The Massachusetts Data Breach Law and Data Security Regulations Protect Consumers from Data Breaches.

Massachusetts has among the strongest data protection laws nationally. Together, its laws and regulations require entities that own or license "personal information"² of Massachusetts residents to develop, implement, and maintain minimum security safeguards to protect such

² In Massachusetts, "personal information" is defined by statute to mean 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; or (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* M.G.L. c. 93H, §1 (attached as **Exhibit 2**).

information from foreseeable threats or hazards and from unauthorized access or use.³ If such information is breached, Massachusetts law obligates entities to provide prompt notice to affected residents and state agencies, including the Attorney General.⁴

My Office has ten years of experience enforcing these laws to protect consumers from data breaches and violations of their privacy. Over this time, we have received notice of over 19,000 data breaches, affecting nearly every sector of the economy. We have investigated countless of these incidents, and enforced the laws against multiple entities that fail to employ reasonable safeguards in the face of foreseeable threats to consumer's personal information. Because of this work, Massachusetts is regarded as a leader in protecting the security and privacy of consumer data.

B. The Massachusetts Attorney General Seeks to Hold Equifax Accountable.

Measured against this enforcement experience, the Equifax breach is one of the worst we have seen. That is why our Office has filed the nation's first enforcement suit against Equifax. We seek to hold Equifax accountable and seek redress for consumers.

As this Committee has previously learned, from March 7, 2017 through July 29, 2017, Equifax left sensitive and private consumer information exposed to intruders by relying on outdated versions of computer code ("Apache Struts") that it knew or should have known was vulnerable to exploitation. Still unknown third parties infiltrated Equifax's computer system through the company's public, online "Dispute Portal." The hackers were present in Equifax's system from at least May 13, 2017 through the end of July 2017.

This computer code vulnerability was publicly known and fixes were posted on at least two U.S. Government websites, among other industry sources. Nonetheless, we allege that Equifax failed to implement the recommended fixes or other steps to prevent the hackers from gaining access.

As a result, we allege that hackers were able to get into Equifax's internal network. But this is not the only thing that we allege Equifax did wrong. Once inside, the hackers were able to roam freely in Equifax's network for months, without Equifax noticing their presence or kicking them out. Over this time, the hackers gained access to hundreds of millions of data records consisting of the most sensitive personal data of 145 million American – all without Equifax noticing.

In our Complaint, we claim that Equifax did not develop, implement, or maintain safeguards required by Massachusetts law to protect consumer data. Such minimum safeguards relate to, among other things, the installation of software security patches, the regular monitoring of computer systems, and the detection and prevention of security systems failures. We also allege that Equifax violated Massachusetts law by keeping hundreds of millions of records containing

³ See M.G.L. c. 93I and Title 201 of the Code of Massachusetts Regulations, section 17.00 *et seq.* (201 C.M.R. 17.00 *et seq.*) (attached as **Exhibit 3** and **Exhibit 4**).

⁴ See M.G.L. c. 93H (**Exhibit 2**).

consumers' sensitive personal information in unencrypted form and not protected through other methods.

The Equifax breach is notable because of its scope, but it is not unique. Data breaches remain a threat to consumers and businesses alike. All too often, we see data breaches that result when a company fails to develop a security program, fails to comply with its security policies, ignores security warnings, neglects to apply critical software patches, or fails to take other reasonable measures to safeguard consumers' information. These all-too-common security lapses are inevitably exploited by cybercriminals hunting for personal information. In brief, our experience shows that there is much room for improvement.

C. To the Extent Any Federal Data Security Standard is Considered, It Should Not Preempt or Undercut State Law.

The Equifax breach may bring into consideration whether a national data breach notice and data security standard is warranted. As noted, Massachusetts has among the strongest data security and breach laws in the country. My Office has serious concerns to the extent any federal standard seeks to set weaker standards than those that currently exist for Massachusetts consumers and that would preempt existing or future state law in this field. States are active, agile, and experienced enforcers of their consumers' data security and privacy, and need to continue to innovate as new risks emerge.

To the extent any such national standard is considered, it must contain strong, minimum data security standards that do not erode existing state protections. As described in more detail in prior comments to the U.S. House Subcommittee on Commerce, Manufacturing, and Trade in March 2015 (attached as **Exhibit 5**), any national standard should, at a minimum:

- Serve as a floor of protections that a state may exceed;
- Contain strong, defined, but flexible data security standards;
- Ensure sufficient enforcement mechanisms, including by State Attorneys General;
- Contain meaningful penalty provisions to deter future violations and ensure violations of the law are not treated simply as the cost of doing business;
- Impose clear requirements for timely and effective consumer notice procedures; and
- Preserve the ability of consumers to seek legal redress for damages for losses resulting or caused by a breach, including minimum statutory damages, as ascertaining individual losses may not be possible or practical.

Given the near-constant threat of data breaches to every American consumer and the risks consumers now face due to the Equifax breach, any national standard must preserve the current level of protections enjoyed by consumers and the enforcement powers of the State Attorneys General to avoid lowering the bar of security and breach standards, and an associated drop in consumer confidence in the marketplace. I respectfully refer the Committee to the standards

outlined in the Massachusetts Data Breach Notice Law (M.G.L. c. 93H) and the Massachusetts Data Security Standards (201 C.M.R. 17.00 *et seq.*) as a model for any national standard.

III. Consumers Need More Meaningful and Accessible Protections When Their Data is Breached.

We allege in our complaint that not only did Equifax fail to prevent a foreseeable breach, it also failed to notify consumers promptly and erected unnecessary hurdles in offering the assistance necessary for consumers to protect themselves from Equifax's own mistakes.

As we allege, the company knew about the breach around July 29, 2017 and should have known then or soon after it had a notification obligation under Massachusetts law, yet it did not notify the Commonwealth or consumers until September 7, 2017. This nearly six-week delay gave the hackers plenty of time, even after they could no longer access Equifax's systems, to use the stolen data before consumers could take steps to protect themselves, such as by freezing their credit files.

We further allege that Equifax compounded this risk by failing to make readily available various protections it was uniquely positioned to offer consumers to mitigate the risk of harm caused by its own mistakes. It charged consumers to place security freezes,⁵ refused to arrange for free security freezes at other national CRAs, failed to offer consumers free credit and fraud monitoring beyond one year, and failed to ensure adequate call center staffing and availability of online services in the days following the announcement of the breach.

We have also already begun to receive complaints of identity theft and fraud. Because identity theft can strike at any time, it is reasonable to assume that consumers will be subject to this risk for years.

The aftermath of the Equifax breach highlights numerous areas for policy development and reform to better protect consumers from the increasing risk of data breaches. Some basic reforms we have proposed on the state level include **free and fast security freezes**. Consumers must be able to easily and quickly freeze their credit files to prevent new accounts from being opened in their names, and they should not pay a penny for a company's data security mistakes.

Similarly, there should be a **"one-stop shop" for security freezes**. We have heard from numerous consumers of the frustrating difficulties they faced in navigating the security freeze processes at the three separate CRAs after the Equifax breach. Section 605A of the Federal Fair Credit Report Act obligates a CRA that receives a request for a fraud alert to notify all other CRAs of that alert. A similar mechanism for a "one-stop shop" should be mandated for security freezes.

⁵ A security freeze is a mechanism by which a CRA prevents a party from accessing a consumer's credit file without the consumer's consent. It is an important protection to consumers whose personal information is compromised in a data breach because it makes it more difficult for an identity thief to open new accounts in a consumer's name. Massachusetts law permits, but does not require, a 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* M.G.L. c. 93, § 62A.

Consumers should also get access to more **free copies of credit reports after a data breach**. Despite the increasing prevalence of data breaches, consumers are unable to monitor their credit reports for free when their information is compromised by a breach. Instead, consumers must use up their one free annual report to check for fraud after being notified of a breach, or pay the CRA for additional reports. This should be changed. Consumers should have free access to their credit reports after a breach to monitor and respond to evidence of unauthorized activity.

If a CRA is breached, it should provide consumers with **free, “no strings attached” credit monitoring for at least five years**. CRAs maintain vast volumes of the very consumer data sought by criminals to commit identity theft and financial fraud. They are also uniquely positioned to monitor consumers’ credit files for such unlawful activities. Given this, they should be required to provide free credit monitoring for consumers affected by a breach at their organization for at least five years. Further, a CRA should not profit from such credit monitoring and consumers should not be required to waive any legal rights – including the right to bring a private action – for availing themselves of the service.

Finally, consumers must be able to **seek full legal redress for any damages** resulting from the data breach, including but not limited to financial losses from identity theft. Entities that allow consumers’ information to be compromised should not be allowed to compel consumers to arbitrate their claims. Consumers must also be able to seek legal redress for losses resulting or caused by a breach, including minimum statutory damages, as ascertaining individual losses may not be possible or practical.

IV. Consumers Need More Control Over How Their Data is Used by the Consumer Reporting Industry.

The Equifax breach raises the larger problem that consumers lack control and knowledge over how the consumer reporting industry is collecting and using their personal data. According to Equifax, the compromised data was not within Equifax’s core consumer or commercial credit reporting databases, but was a different cache of data, stored separately. It is not yet clear how Equifax obtained this consumer data, why they had it, what it was used for, and with whom it was shared. A theme of the anger and confusion consumers have expressed to our Office relates to how Equifax could have had their personal data in the first place, where the consumer had no knowing relationship with Equifax, and made no knowing decision to give it their data.

Consumers’ personal data is their own. Consumers need and deserve control and choice over who has their data. Where decisions of socio-economic consequence are made based on that data, consumers should be aware of what data is disclosed, to whom, and for what purposes. States are on the front lines of consumers’ privacy protection, and are best positioned to innovate in this area. At the state level, we are proposing legislation that would require companies to get a consumer’s prior written permission before accessing his or her credit report or credit score. In our view, this is a modest step to ensure consumers have more control over their information so that they can make smarter decisions about who has it and for what ends it is being used. To the extent federal policy along the above lines is not contemplated, then the Federal Fair Credit Reporting Act should be amended to give the States more freedom to enact stronger protections for its consumers.

V. Conclusion

I appreciate this opportunity to share these views with the Committee, and thank the Committee for its careful examination of these important issues. Please do not hesitate to contact me for any additional detail, clarity or with any questions you may have.

Exhibit 1

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CIVIL ACTION NO.

COMMONWEALTH OF MASSACHUSETTS,

Plaintiff,

v.

EQUIFAX, INC.

Defendant.

COMPLAINT

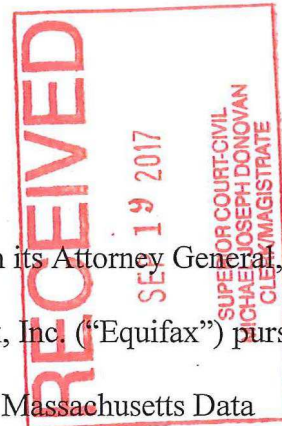
JURY TRIAL REQUESTED

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 warranties of any kind, including warranties 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 77 and 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*

Exhibit 2

PART I ADMINISTRATION OF THE GOVERNMENT
(Chapters 1 through 182)

TITLE XV REGULATION OF TRADE

CHAPTER 93H SECURITY BREACHES

Section 1 Definitions

Section 1. (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.

PART I ADMINISTRATION OF THE GOVERNMENT
(Chapters 1 through 182)

TITLE XV REGULATION OF TRADE

CHAPTER 93H SECURITY BREACHES

Section 2 Regulations to safeguard personal information of commonwealth residents

Section 2. (a) The department of consumer affairs and business regulation shall adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth. Such regulations shall 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.

PART I ADMINISTRATION OF THE GOVERNMENT
(Chapters 1 through 182)

TITLE XV REGULATION OF TRADE

CHAPTER 93H SECURITY BREACHES

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

Section 3. (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) 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.

PART I ADMINISTRATION OF THE GOVERNMENT
(Chapters 1 through 182)

TITLE XV REGULATION OF TRADE

CHAPTER 93H SECURITY BREACHES

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

Section 4. 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.

PART I ADMINISTRATION OF THE GOVERNMENT
(Chapters 1 through 182)

TITLE XV REGULATION OF TRADE

CHAPTER 93H SECURITY BREACHES

Section 5 Applicability of other state and federal laws

Section 5. 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.

PART I ADMINISTRATION OF THE GOVERNMENT
(Chapters 1 through 182)

TITLE XV REGULATION OF TRADE

CHAPTER 93H SECURITY BREACHES

Section 6 Enforcement of chapter

Section 6. 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.

Exhibit 3

PART I ADMINISTRATION OF THE GOVERNMENT
(Chapters 1 through 182)

TITLE XV REGULATION OF TRADE

CHAPTER 93I DISPOSITIONS AND DESTRUCTION OF RECORDS

Section 1 Definitions

Section 1. 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.

PART I ADMINISTRATION OF THE GOVERNMENT
(Chapters 1 through 182)

TITLE XV REGULATION OF TRADE

CHAPTER 93I DISPOSITIONS AND DESTRUCTION OF RECORDS

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

Section 2. 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.

PART I ADMINISTRATION OF THE GOVERNMENT
(Chapters 1 through 182)

TITLE XV REGULATION OF TRADE

CHAPTER 93I DISPOSITIONS AND DESTRUCTION OF RECORDS

Section 3 Enforcement

Section 3. 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.

Exhibit 4

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH

Section:

17.01: Purpose and Scope

17.02: Definitions

17.03: Duty to Protect and Standards for Protecting Personal Information

17.04: Computer System Security Requirements

17.05: Compliance Deadline

17.01 Purpose and Scope

(1) Purpose

This regulation 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. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. The objectives of this regulation 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.

(2) Scope

The provisions of this regulation apply to all persons that own or license personal information about a resident of the Commonwealth.

17.02: Definitions

The following words as used herein 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 this regulation.

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 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; 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 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.

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.

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.

REGULATORY AUTHORITY

201 CMR 17.00: M.G.L. c. 93H

EXHIBIT 5



MAURA HEALEY
ATTORNEY GENERAL

THE COMMONWEALTH OF MASSACHUSETTS
OFFICE OF THE ATTORNEY GENERAL

ONE ASHBURTON PLACE
BOSTON, MASSACHUSETTS 02108

TEL: (617) 727-2200
WWW.MASS.GOV/AGO

March 17, 2015

The Honorable Michael C. Burgess M.D.
Chairman
Subcommittee on Commerce,
Manufacturing, & Trade
Energy and Commerce Committee
U.S. House of Representatives
Washington, DC 20215

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce,
Manufacturing, & Trade
Energy and Commerce Committee
U.S. House of Representatives
Washington, DC 20215

Re: *The Data Security and Breach Notification Act of 2015*

Dear Chairman Burgess and Ranking Member Schakowsky:

We write to address the discussion draft bill entitled the Data Security and Breach Notification Act of 2015 (the "Bill"), dated March 12, 2015, which seeks to establish federal standards concerning data security and data breach notification obligations. We appreciate that the Committee recognizes the importance of strong data security protections and breach disclosure obligations to protect consumers and preserve consumer confidence in the market. Moreover, we are cognizant of the business community's concerns regarding compliance with myriad state security breach notification regimes.

Nonetheless, we write to express serious reservations with the Bill, which in our view represents an unnecessary retraction of existing protections for consumers at a time when such protections are imperative. Our concerns are informed by this Office's experience enforcing Massachusetts' data security breach notification law (Mass. Gen. Law ch. 93H, attached as [Exhibit 1](#)), data security regulations (Title 201 of the Code of Massachusetts Regulations ("CMR"), section 17.00 *et seq.*, attached as [Exhibit 2](#)), and data disposal law (Mass. Gen. Law ch. 93I, attached as [Exhibit 3](#)). Together, these laws and regulations – which are enforced by this Office through the Massachusetts Consumer Protection Act¹ – require entities that own or license "personal information"² of Massachusetts residents to develop, implement, and maintain

¹ Mass Gen. Law ch. 93A.

² In Massachusetts, "personal information" is defined by statute to mean 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

minimum security procedures and policies consistent with industry standards to safeguard such information (whether in paper or electronic form) from anticipated threats or hazards and from unauthorized access or use.³ Massachusetts law also obligates entities to provide prompt notice to affected residents and state agencies in the event of a breach of security or compromise of that information.⁴ These laws and regulations protect consumers from identity theft and fraud, and concomitantly, instill consumer confidence in the commercial collection and use of their personal information.

From January 1, 2008 through July 31, 2014, this Office received notice pursuant to Mass. Gen. Law ch. 93H, section 3 of over 8,665 security breaches, affecting nearly 5 million Massachusetts residents. To the extent any of those breaches resulted in enforcement actions by this Office (a very small percentage), the circumstances reflected gross failures to implement or maintain basic security practices, unreasonable delays in providing notice of the breach, or other egregious conduct that raised real risks of resulting consumer harm. As a result, this Office has an informed and comprehensive view into the nature, extent, and frequency of data breaches, the risks faced by consumers, and the security practices and procedures that can prevent or mitigate those risks.

Accordingly, this Office is uniquely positioned to highlight some of the potential problems with the Bill. Our principal concerns are as follows:

I. The Bill's proposed preemption of state law undercuts existing consumer protections and is overly broad.

Although the stated purpose of the Bill is to “protect consumers from identity theft, economic loss or economic harm, and financial fraud,” the Bill would preempt Massachusetts’ data security/breach law to the extent they relate to data in electronic form, and replace it with weaker protections. In addition, the Bill would preempt other state laws that protect “data in electronic form” from unauthorized access (including, among others, laws that criminalize the interception of wire communications (Mass Gen. Law c. 272, § 99(C)) or require the confidentiality of medical records and mental health records (Mass Gen. Law c. 111, § 70E(b), and c. 123, § 36)). It is also in conflict with, and would appear to potentially preempt, the enforcement authority given to the States under other federal laws relating to the security of electronic data (including, for example, the Health Information Technology for Economic and Clinical Health (HITECH) Act (42 U.S.C. 1320d–5(d)). Such sweeping preemption is harmful to consumers, and restricts innovative States from responding to and protecting their residents from emerging threats to the privacy and security of their data. The Bill should at least preserve the current level of protections enjoyed by consumers and the enforcement powers of the state Attorneys General to avoid a national downward harmonization of security and breach standards, and an associated drop in consumer confidence in the marketplace. The Bill will not only fail to

number; or (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. Law ch. 93H, §1.

³ See Mass Gen. Law ch. 93I and 201 CMR 17.00 *et seq.*

⁴ See Mass Gen. Law ch. 93H.

maintain consumer confidence in the marketplace, but will scale back the protections consumers currently enjoy.

II. Minimum data security standards are important and necessary, but the proposed standards leave consumers' data vulnerable.

We agree that establishing minimum data security standards is important and necessary. Massachusetts has had robust minimum data security regulations in place since 2010 in the form of data security regulations (201 CMR 17.00 *et seq.*) and data disposal law (Mass Gen. Law ch. 93I). The flexible standards established by Massachusetts represent the leading information security framework in the nation, and are the standards to which all commercial entities aspire.⁵ We are concerned the Bill will lower the bar already set by Massachusetts and other existing federal data security regulations,⁶ and will weaken consumers' confidence in the security of their personal information in commerce. Specifically, the Bill fails to articulate the minimum data security standards that would constitute the required "reasonable security measures and practices." As a result, the Bill would result in the retroactive establishment of data security standards through protracted litigation and piecemeal judicial interpretation. To ensure that the data security obligations are sufficiently robust, defined, and responsive to changing threats and technologies, the Bill should establish minimum data security standards, modeled after those in place in Massachusetts and under existing federal law.

III. The Bill fails to require notice that will ensure meaningful enforcement.

While the Bill's requirement of notice of a breach to the Federal Trade Commission is an important first step for enforcement of the Bill's requirements, it is not by itself enough. Recent breaches reported in the media underscore the necessary role played by the state Attorneys General in enforcing data breach and data security requirements. The absence of a requirement to provide notice to state Attorneys General of data breaches – even for those breaches that impact a significant number of their residents – frustrates their ability to protect their residents. Further, the threshold for providing notice to the FTC may be set too high. In Massachusetts, the vast majority (approximately 97%) of the 2,314 data breaches reported in 2013 involved fewer than 10,000 persons; each of these breaches affected, on average, 74 persons. Assuming these statistics are consistent nationally, the Bill would create an enforcement "blind spot" for both

⁵ Similar to existing federal standards applicable to financial institutions (*see* 16 C.F.R. Part 314) and entities covered under HIPAA (*see e.g.* 45 CFR Subpart C of Part 164), Massachusetts requires entities to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of personal information (201 CMR 17.03(2)(b)); develop, implement and maintain a "written comprehensive information security program" containing physical, administrative and technical safeguards necessary to protect personal information from those risks (201 CMR 17.03); take reasonable steps to oversee third parties handling personal information (201 CMR 17.03(2)(f)); and securely dispose of personal information (Mass Gen. Law ch. 93I). Cognizant of the particular risks associated with electronic data, Massachusetts also requires entities, among other things, to establish and maintain a technically-feasible computer security system (201 CMR 17.04); and to encrypt personal information sent over public networks or wirelessly, or stored on laptops and portable devices (201 CMR 17.04(3), (5)).

⁶ *See, e.g.*, 16 C.F.R. Part 314 (Standards for Safeguarding Customer Information); 45 CFR Subpart C of Part 164 (Security Standards for the Protection of Electronic Protected Health Information); 16 CFR Part 682 (Proper Disposal of Consumer Information); and 201 CMR 17.00 *et seq.* (Standards for the Protection of Personal Information of Residents of the Commonwealth).

state and federal regulators, who would not receive notice of the vast majority of data breaches that occur. To ensure effective enforcement of the Bill, the Bill should require prompt notice of breaches to the FTC and also to the state Attorneys General in cases where their State's residents are impacted.

IV. The Bill infringes on the States' consumer protection enforcement authority.

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 from that action if the FTC initiates the action first. Such requirements infringe on the enforcement prerogatives of the state Attorneys General by injecting unnecessary delay and costs, and unnecessarily complicating their efforts to enforce their respective consumer protection laws. Numerous federal laws illustrate that dual federal/state enforcement coordination of consumer protection laws is both possible and effective, including for example: the Federal Trade Commission Act (15 U.S.C. § 45(a)(1) and its numerous State counterparts (*see, e.g.* Mass Gen. Law ch. 93A), the Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*), 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.*). To ensure meaningful protections for consumers, the Bill should likewise establish a dual federal/state enforcement framework that respects – not constricts - the enforcement prerogative of the States.

V. The penalties proposed by the Bill are insufficient, and leave consumers without a remedy.

The Bill limits the state Attorneys General to civil penalties of up to \$11,000 for each day per violation of the Bill's information security requirements, and up to \$11,000 per violation of the Bill's breach notice requirements, capped at a total liability of \$2.5 million, and based on "penalty factors" that do not expressly take into account consumer harm or the need to deter future violations. Given the massive scope of recently-reported breaches affecting some of the largest companies in the country, a civil penalty cap of \$2.5 million may be an insufficient deterrent, and could be treated as a cost of doing business. Moreover, the Bill does not authorize the state Attorneys General to recover consumer restitution, and further does not provide for a private cause of action. Thus, a consumer who suffers loss due to a data breach effectively has no remedy under this Bill. The Bill should instead retain the existing discretion of state Attorneys General and the FTC to seek both civil penalties and consumer restitution at levels sufficient to penalize and deter the conduct at issue and make consumers whole, and further provide a private right of action.

VI. The Bill's data breach notice obligations lack many key safeguards.

Requiring prompt notice to consumers affected by a breach and to state regulators serves important ends, including alerting consumers to the fact that their personal information may be at risk, educating the market as to existing or emerging security threats, and providing incentives for improving security practices to prevent breaches. The data breach notice standards proposed by the Bill fall short for a number of reasons.

First, the Bill allows entities to delay notice without regard to the risks faced by consumers. By requiring notice only when the entity both “discovers” a “breach of security” and “determines” that a “reasonable risk of” identity theft, economic loss or harm, or financial fraud has resulted or will result, the Bill creates a disincentive for an entity to monitor their systems for potential compromises or vulnerabilities, an outcome directly at odds with the Bill’s stated purposes. Once “discovered,” the Bill would further grant a covered entity an unspecified (and unlimited) period of time to “tak[e] the necessary measures” to “determine the scope of the breach of security and restore the reasonable integrity, security, and confidentiality” of its data system. This creates opportunities for delay that would undermine the force of the proposed thirty (30) day notification deadline, and which may subject consumers to unnecessary risk. If preventing identity theft is the goal, notice should be issued in time for consumers to protect themselves, even if the breached entity has not completed its investigation or is still in the process of restoring its systems.

Second, the Bill fails to require notice in cases where identity theft is a real risk, such as when personal information is accessed or acquired with authorization (*e.g.* by an authorized employee) but used for unauthorized purposes. Additionally, the Bill does not provide for notice in cases where encrypted personal information – and information allowing for the decryption of that information – are both compromised in the breach.

Third, because notice obligation under the Bill turns on the manner in which a covered entity deals with the personal information, rather than its legal relationship to it,⁷ notice could be delayed or avoided as a result of disputes between covered entities as to which is the “third-party entity” and which is the covered entity responsible for notice. It may also result in consumer confusion insofar as consumers may receive notice from an entity with which they have not had direct dealings. To avoid such results, the Bill should follow Massachusetts’ lead and impose the consumer notification duty on the entity that “owns or licenses” the breached personal information. In turn, entities that “maintain or store” the breached personal information should be obligated to promptly notify the owner or licensor. *See* Mass Gen. Law ch. 93H, §§ 3(a), (b).

Finally, the content and form of the required consumer notice lacks several key safeguards. The Bill does not require the notice to contain information as to how a consumer may protect him or herself and instead, directs the consumer to the FTC for more information. The Bill should require the consumer notice to contain the information necessary for the consumer to protect him/herself from identity theft.⁸ In cases where “substitute notice” is

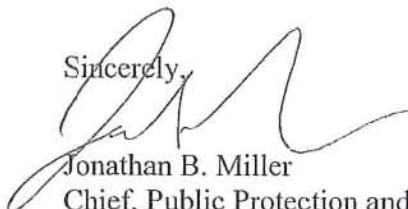
⁷ The Bill imposes the consumer notice obligation on “a covered entity that uses, accesses, transmits, stores, disposes of, or collects” personal information (section 3(a)(1)), but not on the covered entity that “store[s], processe[s], or maintain[s]” personal information” for a covered entity. This “third-party entity” would “ha[ve] no other notification obligations” than to notify the covered entity for whom it stores, processes, or maintains the personal information (section 3(b)(1)(A)).

⁸ Such information should include, for example, information concerning the availability of security freezes, the importance of filing and obtaining a police report (information required under Mass Gen. Law ch. 93H, § 3), the availability of fraud alerts, the importance of monitoring one’s credit reports, and other information about the breach that would allow the consumer to fairly assess their risk and protect themselves.

authorized, the entity should be required to make a media posting sufficient to constitute legal notice of the breach.⁹

We appreciate this opportunity to convey our serious 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.

Sincerely,



Jonathan B. Miller
Chief, Public Protection and Advocacy Bureau

Sara Cable
Assistant Attorney General
Consumer Protection Division

Office of Attorney General Maura Healey
Commonwealth of Massachusetts
One Ashburton Place
Boston, MA 02108
(617) 727-2200

⁹ See, e.g. Mass Gen. Law ch. 93H, § 1 (requiring as one component of substitute notice “publication in or broadcast through media or medium that provides notice throughout the commonwealth [of Massachusetts]”).