COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CIVIL ACTION NO.

COMMONWEALTH OF MASSACHUSETTS,

Plaintiff,

v.

EQUIFAX, INC.

Defendant.

COMPLAINT

JURY TRIAL REQUESTED

INTRODUCTION

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

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

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

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

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

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

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

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

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

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

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

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

THE PARTIES

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

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

JURISDICTION, AUTHORITY, AND VENUE

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

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

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

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

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

FACTS

Equifax's Business

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

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

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

The Data Breach

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

54. Equifax also failed to comply with Massachusetts Law.

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

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

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

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

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

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

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

Equifax Delayed Notifying the Public of the Data Breach

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

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

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

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

66. Under chapter 93H, § 1, a breached entity may provide "substitute notice" to consumers "if the person . . . required to provide notice demonstrates that the cost of providing

written notice will exceed $250,000, or that the affected class of Massachusetts residents to be notified exceeds 500,000 residents, or that the person . . . does not have sufficient contact information to provide notice." Substitute notice consists of all three of the following: (1) email notice to the extent the entity has email addresses for the affected residents, (2) a "clear and conspicuous posting of the notice on the home page" of the notifying entity and (3) "publication in or broadcast through media or medium that provides notice throughout the commonwealth." G.L. c. 93H, §1.

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

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

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

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

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

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

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

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

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

---

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

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

[4] Id. at 8.

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

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

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

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

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

CAUSES OF ACTION

COUNT I

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

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

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

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

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

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

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

> [A] [Massachusetts] resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account . . . .

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

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

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

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

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

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

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

COUNT II

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COUNT III

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

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

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

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

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

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

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

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

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

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

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

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

COUNT IV

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

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

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

Policy that it has:

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

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

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

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

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

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

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

COUNT V

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

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

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

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

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

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

PRAYER FOR RELIEF

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

1. Enter a permanent injunction prescribing appropriate relief;

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

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

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

REQUEST FOR JURY TRIAL

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

Respectfully submitted,

COMMONWEALTH OF MASSACHUSETTS

MAURA HEALEY
ATTORNEY GENERAL

By: _____

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

Date: September 19, 2017