

**IN THE CIRCUIT COURT OF COOK COUNTY  
COUNTY DEPARTMENT, CHANCERY DIVISION**

**CITY OF CHICAGO,**  
  
**Plaintiff,**

**v.**

**EQUIFAX INC.,**  
  
**Defendant.**

2017CH13047  
CALENDAR/ROOM 07  
TIME 00:00  
General Chancery

**JURY TRIAL DEMANDED**

**COMPLAINT**

The City of Chicago (“Chicago”), by its Corporation Counsel, Edward N. Siskel, files this Complaint under the Consumer Fraud, Unfair Competition or Deceptive Practices Ordinance (“Ordinance”), § 2-25-090 of the Municipal Code of Chicago (“MCC”), against Equifax Inc. (“Equifax”), seeking relief against Equifax on behalf of Chicago and its residents for Equifax’s deceptive and unfair business practices committed while conducting business in Chicago and in support states as follows:

**INTRODUCTION**

1. Equifax is one of three primary companies in the United States providing consumer reporting, credit monitoring, and identity theft protection services. Equifax collects and maintains data and personal information regarding more than 820 million individuals worldwide, including Chicago residents. The personal data that Equifax gathers and maintains affects virtually every aspect of an individual’s profile in the marketplace, and includes, but is not limited to, their names, addresses, social security numbers, as well as bank, credit and other financial account information.

2. Equifax serves as a virtual gatekeeper for access to credit markets, and more broadly, to socioeconomic opportunity and advancement. Every day, businesses across the

FILED-7  
2017 SEP 28 AM 8:57  
DOROTHY BROWN

country rely on Equifax's credit profiles to make decisions as to the credit-worthiness of consumers. The information that Equifax gathers, maintains, and disseminates to its customers impacts many of the most important decisions in the lives of members of the public, such as whether they can buy a house, obtain a loan, obtain credit at favorable interest rates and terms, lease a vehicle, or even get a job or cellphone service.

3. Members of the public do not voluntarily choose to give their sensitive personal consumer information to Equifax, and they must rely on Equifax to protect their information, and to prevent it from being accessed inappropriately. Equifax controls how, when, and to whom the data it stockpiles is disclosed. Accordingly, it was and is incumbent on Equifax to implement and maintain the strongest safeguards to protect that data. Equifax has failed to do so.

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

5. As a result, criminals were able to access Equifax's computer system from at least May 13, 2017 through July 30, 2017, and according to Equifax's own estimates, reportedly stole sensitive and personal information of 143 million members of the public, approximately 44% of the United States population ("Data Breach"). The affected individuals include an estimated 5.4 million people who reside in Illinois, which includes residents of Chicago. The Data Breach, which Equifax first disclosed to the public on September 7, 2017, exposed to still-unknown persons

the most sensitive personal and financial data of Chicago residents, including full names, social security numbers, dates of birth, addresses, and for some, credit card numbers, driver's license numbers, and/or other personally-identifiable information.

6. Equifax could and should have prevented the Data Breach by implementing and maintaining reasonable safeguards, consistent with representations Equifax made to the public in its marketing materials and privacy policies, and compliant with industry standards, best practices, and the requirements of Illinois state and Chicago municipal law. Equifax failed to do so.

7. By failing to secure information, Equifax exposed many residents of Chicago to the risks of identity theft and financial fraud, tax return scams, theft from their bank accounts, health identity fraud, and other potential harm.

8. Affected members of the public, including Chicago residents, have spent, and will continue to spend, money, time, and other resources attempting to protect against the increased risk of identity theft or fraud, including by placing security freezes on 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 subjected Chicago residents to 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 that it gathers, maintains, and disseminates, and the serious consequences when that data is exposed, Equifax's failure to secure this information constitutes a betrayal of public trust and violation of Chicago's Ordinance. As Equifax's own recently-resigned former Chairman and Chief Executive Officer admitted, the Data Breach "strikes at the heart of who we are and what we do." *See* <https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628>.

10. Chicago brings this action to ensure that Equifax is held accountable for its gross failure to protect and secure the personal and sensitive data of Chicago residents, and not allowed to prioritize its revenue stream and profits over the safety and privacy of the public's sensitive and personal data. Chicago seeks civil penalties, restitution, and all necessary, appropriate, and available equitable and injunctive relief to address, remedy, and prevent harm to Chicago residents resulting from Equifax's actions and inactions, as provided by the Ordinance.

### **THE PARTIES**

11. The Plaintiff Chicago is a municipal corporation and a home rule unit of local government organized and existing pursuant to the laws of the State of Illinois.

12. The Defendant Equifax is a publicly-traded Georgia corporation with its principal place of business located at 1550 Peachtree Street N.E., Atlanta, Georgia, registered to do business in the State of Illinois, and doing business in Chicago.

### **JURISDICTION AND VENUE**

13. This Court has jurisdiction over the subject matter of this action, pursuant to 735 ILCS 5/2-209, because the actions that are the subject of this lawsuit took place in Chicago.

14. This Court has personal jurisdiction over Equifax, under 735 ILCS 5/2-209, because Equifax has engaged in business in Chicago, and Equifax's actions and inactions have affected Chicago residents.

15. Venue is proper in Cook County, under 735 ILCS 5/2-101, because the harm giving rise to this claim occurred in Cook County.

### **FACTS**

#### ***Equifax's Business.***

16. Equifax's core business is 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.” See <http://www.equifax.com/about-equifax/company-profile>. Equifax employs approximately 9,900 people worldwide. *Id.*

17. As part of its business, Equifax creates, maintains, and sells “credit reports” and “credit scores” regarding individual consumers, including Chicago 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. A credit score is a proprietary number, derived from a credit report and other information, and is intended to predict whether a person is likely to repay debts.

18. Third parties use credit reports and credit scores to make highly consequential decisions affecting Chicago residents. For example, 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.***

19. At all relevant times, Equifax maintained a publicly available website at [www.equifax.com](http://www.equifax.com).

20. Within that website are various publicly available web pages directed to consumers, including Chicago 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 (“Dispute Portal”).

21. Information about members of the public, including their names, addresses, social security numbers, birth dates, driver’s license numbers, and credit card numbers, was maintained by Equifax in files accessible through the Dispute Portal. This information included “Personal Information,” as defined in Illinois’s Personal Information Protection Act, 815 ILCS 530/5 (“PIPA”). Equifax maintained information about at least 143 million people, including Chicago residents, many of whom had never affirmatively accessed the Dispute Portal.

22. The Personal Information accessible through the Dispute Portal was not encrypted.

23. Between May 13, 2017 and July 30, 2017, unauthorized third parties infiltrated Equifax’s computer system via the Dispute Portal. These parties accessed and likely stole Personal Information from Equifax’s data systems, including Personal Information of Chicago residents.

***Equifax Ignored Numerous Signs that Its System, and the Data Stored Therein, Including Data of Chicago Residents, Was Vulnerable to Hackers.***

24. 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.”

25. Apache Struts is an open source web application framework, designed to support the development of web applications.

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

27. As an “open-source” web framework, 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.

28. At all relevant times, numerous well-known resources have been available to support companies relying on open-source code, including Apache Struts. When notified of a possible security issue, these resources work to quickly develop a solution to the problem, then publicly announce to users that a security vulnerability in the open-source framework exists, explain its risks, and propose fixes.

29. At least four separate organizations published warnings about the vulnerability of Apache Struts to hackers before the Data Breach.

30. For example, the Apache Software Foundation (“Apache”), a non-profit corporation, releases updated versions of Apache Struts to protect or “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.

31. 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 Apache Struts and other open-source code, the risks they pose, and ways to fix them.

32. Likewise, the MITRE Corporation, a “not-for-profit organization that operates research and development centers sponsored by the [United States] federal government,” *see* <https://www.mitre.org/>, 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>.

33. On March 7, 2017, Apache published a 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”). See <https://cwiki.apache.org/confluence/display/WW/S2-045>, and <https://cwiki.apache.org/confluence/display/WW/S2-046>. The vulnerability was assigned the CVE identifier CVE-2017-5638 (“March Security Vulnerability”).

34. The Apache Security Bulletins were directed to “All Struts2 developers and users.” The Apache Security Bulletins warned that the web application framework 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 malicious commands on the website’s server (the computer that stores the information that supports the website).

35. 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. *Id.*

36. NIST also publicized the March Security Vulnerability in its NVD on or about March 10, 2017. See <https://nvd.nist.gov/vuln/detail/CVE-2017-5638> (“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.

37. 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”). See <https://www.us-cert.gov/ncas/bulletins/SB17-079>.

38. Likewise, MITRE included the March Security Vulnerability in its database and documented various external website references to the March Security Vulnerability. See <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638>.

39. Immediately after the public disclosure of the March Security Vulnerability by Apache, media reports claimed that hackers and other criminals had begun actively exploiting the flaw by installing rogue applications on affected web servers of numerous companies, including banks, government agencies, internet companies, and other websites.

40. 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 and other criminals.

41. As of or soon after March 7, 2017, Equifax knew or should have known, based on information available from multiple public sources, including the Apache Security Bulletins, the NIST Notice, the US CERT Alert, and the MITRE database, that the March Security Vulnerability was a critical security vulnerability in the Apache Struts framework.

42. Equifax admitted, through a notice on its website, <https://www.equifaxsecurity2017.com>, that “Equifax’s Security organization was aware of this vulnerability” in the Apache Struts framework in early March 2017.

43. As of or soon after March 7, 2017, Equifax knew or should have known, based on information available from multiple public sources, that the version of Apache Struts it employed on its websites, including the Dispute Portal, was susceptible to the March Security Vulnerability.

44. As of or soon after March 7, 2017, Equifax knew or should have known, based on information available from multiple public sources, that the March Security Vulnerability rendered the Personal Information maintained in its data systems vulnerable to unauthorized access by hackers and other criminals.

45. Despite this knowledge, Equifax continued to use an Apache Struts-based web application that was susceptible to the March Security Vulnerability for its Dispute Portal until at least July 30, 2017.

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

47. In addition, until at least July 30, 2017, Equifax did not detect or appropriately respond to infiltrations by unauthorized parties of its computer systems, and it did not detect or appropriately respond to indications that those unauthorized parties were accessing and likely stealing Personal Information.

48. As a result of Equifax’s actions and failures to act, the Data Breach occurred, and hackers and other criminals were able to access and steal the sensitive and personal data of 143 million members of the public, including the Personal Information of Chicago residents.

***Equifax's Security Program Fell Short of Its  
Promises to the Public, as well as Illinois and Chicago Law.***

49. At all relevant times, Equifax promised the public that safeguarding their sensitive, personal information was “a top priority.” At all relevant times in its Privacy Policy, available through a hyperlink at the bottom of each page of its public website, Equifax represented to the residents of Chicago:

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.

50. Equifax was aware of the risks associated with identity theft. On its website, Equifax lists “some of the ways identity theft might happen,” including when identity thieves “steal electronic records through a data breach.”

51. Equifax likewise represented to the public that it would keep all of their credit information secure, including information people submitted through the Dispute Portal. 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.”

52. Equifax intended that the public, including Chicago residents, rely on its deceptive representations and communications regarding the security of Personal Information.

53. By failing to patch or otherwise resolve the March Security Vulnerability, detect hackers and other criminals in its network, prevent those criminals from accessing and stealing Personal Information, and otherwise failing to safeguard Personal Information, as set forth herein, Equifax failed to fulfill its representations to the public and the residents of Chicago.

54. Equifax also failed to comply with Illinois state and Chicago municipal law.

***Equifax Delayed Notifying the Public, Including Chicago Residents, of the Data Breach.***

55. Illinois's Personal Information Privacy Act, 815 ILCS 530/1 *et seq.*, required Equifax to provide timely notice to Chicago residents of the Data Breach. Section 10 of PIPA, 815 ILCS 530/10, provides:

(a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. *The disclosure notification shall be made in the most expedient time possible and without unreasonable delay*, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

815 ILCS 530/10(a) (emphasis added).

56. The Ordinance provides that any "unlawful practice" under the Illinois Consumer Fraud and Deceptive Business Practices Act constitutes a violation of the Ordinance. MCC § 2-25-090. A violation of Illinois's PIPA "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act." 815 ILCS 530/20. Thus, any violation of PIPA constitutes a violation of the Ordinance.

57. Equifax is a data collector that owns or licenses personal information concerning Illinois, including Chicago, residents.

58. Timely notification by Equifax, as required by PIPA, was particularly important because many Chicago residents were not aware that their Personal Information was compromised. Because Equifax obtains Personal Information from banks, credit card issuers, retailers, lenders, and public records, many members of the public are not aware that Equifax has collected and retained their Personal Information.

59. As of or soon after July 30, 2017, Equifax knew or should have known that a breach of the security of its system data had occurred. Equifax failed to notify Chicago residents

of the breach in the most expedient time possible and without unreasonable delay, in violation of both PIPA and the Ordinance.

60. Section 10 of PIPA also specifies the required content of the disclosure notification:

The disclosure notification to an Illinois resident shall include, but need not be limited to, information as follows:

(1) With respect to personal information as defined in Section 5 in paragraph (1) of the definition of “personal information”:

(A) the toll-free numbers and addresses for consumer reporting agencies;

(B) the toll-free number, address, and website address for the Federal Trade Commission; and

(C) a statement that the individual can obtain information from these sources about fraud alerts and security freezes.

(2) With respect to personal information defined in Section 5 in paragraph (2) of the definition of “personal information”, notice may be provided in electronic or other form directing the Illinois resident whose personal information has been breached to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer.

61. As of the date of filing of this Complaint, Equifax has failed to provide the disclosure notifications to Chicago residents required by Section 10 of PIPA and the Ordinance.

***Equifax’s Actions and Inactions in Connection with the Data Breach Have Created, Compounded, and Exacerbated the Harms Suffered by the Public, Including Chicago Residents.***

62. Chicago is not required to demonstrate harm to its residents in order to enforce the Ordinance.

63. Nevertheless, Chicago residents 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.

64. 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—hackers and criminals 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.

See <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft>.

65. Identity theft results in real financial losses, lost time, and aggravation to Chicago residents.

66. In its 2014 Victims of Identity Theft report, the United States Department of Justice stated that 65% of the over 17 million identity theft victims that year suffered a financial loss, and 13% of the total identity theft victims never had those losses reimbursed. See U.S. Dept. of Justice, Bureau of Justice Statistics, Victims of Identity Theft 2014, at 6 & Table 6, *available at* <http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5408>. The average out-of-pocket loss for those victims was \$2,895.

67. Identity theft victims also "paid higher interest rates on credit cards, they were turned down for loans or other credit, their utilities were turned off, or they were the subject of criminal proceedings." *Id.* at 8. The report also noted that more than one-third of identity theft victims suffered moderate or severe emotional distress due to the crime. See *id.* at 9, Table 9.

68. The Data Breach has substantially increased the risk that the affected Chicago residents will be victims of identity theft or financial fraud at some unknown point in the future.

69. In order to protect themselves from this increased risk of identity theft and fraud, many Chicago residents have placed or 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 resident’s consent.

70. As a result of Equifax’s actions and failures to act in connection with the Data Breach, and in an effort to protect themselves against identity theft or financial fraud, many Chicago residents 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.

71. Further, Equifax has complicated Chicago residents’ 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 Chicago residents whether they were affected by the Data Breach, has charged consumers to place security freezes (and presumably unfairly profited thereby), has failed to offer Chicago residents 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 Chicago residents.

***Even After the Data Breach, Equifax Engaged in Further Unfair and Deceptive Conduct.***

72. In response to the Security Breach, on September 7, 2017, Equifax established an allegedly dedicated secure website (<https://www.equifaxsecurity2017.com>), where members of the public, including Chicago residents, could check to see if their “personal information was

potentially impacted,” and offered consumers one year of “complimentary identity theft protection and credit file monitoring” through an Equifax product, TrustedID Premier. See

<https://web.archive.org/web/20170909111630/https://www.equifax.com/personal/>.

73. However, before anyone could avail themselves of Equifax’s “complimentary offer,” they were first required to agree to TrustedID Premier’s “Terms of Use,” which included waiving their rights to participate in a class action, and submitting to binding individual arbitration, “even if the facts and circumstances upon which the claims are based already occurred or existed”:

YOU MUST ACCEPT THIS AGREEMENT, INCLUDING ITS “ARBITRATION” SECTION BELOW, BEFORE YOU WILL BE PERMITTED TO REGISTER FOR, USE OR PURCHASE ANY PRODUCT. BY REGISTERING ON THIS WEBSITE AND SUBMITTING YOUR ORDER, YOU ARE ACKNOWLEDGING ELECTRONIC RECEIPT OF, AND YOUR AGREEMENT TO BE BOUND BY, THIS AGREEMENT. YOU ALSO AGREE TO BE BOUND BY THIS AGREEMENT BY USING OR PAYING FOR OUR PRODUCTS OR TAKING OTHER ACTIONS THAT INDICATE ACCEPTANCE OF THIS AGREEMENT.

\* \* \* \*

**ARBITRATION.** PLEASE READ THIS ENTIRE SECTION CAREFULLY BECAUSE IT AFFECTS YOUR LEGAL RIGHTS BY REQUIRING ARBITRATION OF DISPUTES (EXCEPT AS SET FORTH BELOW) AND A WAIVER OF THE ABILITY TO BRING OR PARTICIPATE IN A CLASS ACTION, CLASS ARBITRATION, OR OTHER REPRESENTATIVE ACTION. ARBITRATION PROVIDES A QUICK AND COST EFFECTIVE MECHANISM FOR RESOLVING DISPUTES, BUT YOU SHOULD BE AWARE THAT IT ALSO LIMITS YOUR RIGHTS TO DISCOVERY AND APPEAL.

See <https://web.archive.org/web/20170908073051/https://trustedidpremier.com/static/terms>.

74. Moreover, if enrollees did not cancel Equifax’s credit monitoring program after one year, their subscription would automatically be renewed, and they would be charged a renewal fee.

75. Further, many individuals were reporting that even when inputting fake or incorrect



information into Equifax's website, those individuals were nonetheless informed that their personal information "may have been impacted," and Equifax encouraged them to sign up for Equifax's "free" services. *See, e.g.,* <https://gizmodo.com/why-some-are-recommending-credit-freezes-in-the-wake-1802924951>.

76. Thus, under the guise of providing very belated assistance to the victims of its Data Breach, Equifax was in fact not even reliably informing members of the public, including Chicago residents, whether their data was in fact affected, while surreptitiously attempting to limit their legal rights, as well as attempting to line its own pockets by automatically renewing enrollees who failed to cancel their "free" subscriptions after one year.

77. Subsequently, only after intense criticism from the media and public officials, on September 11, 2017, Equifax provided a "Progress Update for Consumers," including Chicago residents, on its website, issuing, among other things, the following "clarification":

**Clarification Regarding Automatic Sign-Up to TrustedID Premier**  
We are not requesting consumers' credit card information when they sign up for the free credit file monitoring and identity theft protection we are offering to all U.S. consumers. Consumers who sign up for TrustedID Premier will not be automatically enrolled or charged after the conclusion of the complimentary year of TrustedID Premier.

*See* <https://www.equifaxsecurity2017.com/2017/09/11/progress-update-consumers-2/>.

78. Equifax further informed members of the public, including Chicago residents, that:

We've added an FAQ to our website to confirm that enrolling in the free credit file monitoring and identity theft protection that we are offering as part of this cybersecurity incident does not waive any rights to take legal action. We removed that language from the Terms of Use on the website, [www.equifaxsecurity2017.com](http://www.equifaxsecurity2017.com). The Terms of Use on [www.equifax.com](http://www.equifax.com) do not apply to the TrustedID Premier product being offered to consumers as a result of the cybersecurity incident

*See id.*

## CAUSES OF ACTION

### COUNT I

#### **Failure to Give Prompt Notice of Data Breach – Violation of MCC § 2-25-090**

79. Chicago realleges and incorporates herein by reference each of the foregoing allegations contained this Complaint as though fully alleged in this Count.

80. The Ordinance, MCC § 2-25-090, provides that any “unlawful practice” under the Illinois Consumer Fraud and Deceptive Business Practices Act constitutes a violation of the Ordinance. The Ordinance states, in relevant part:

(a) No person shall engage in any act of consumer fraud, unfair method of competition, or deceptive practice while conducting any trade or business in the city. *Any conduct constituting an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act, as now or hereafter amended, or constituting a violation of Section 7-4-040, Section 7-4-060 or any section of this Code relating to business operations or consumer protection, shall be a violation of this section.* In construing this section, consideration shall be given to court interpretations relating to the Illinois Consumer Fraud and Deceptive Business Practices Act, as amended. In construing this section, consideration shall also be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a) of the Federal Trade Commission Act, 15 U.S.C.A., Section 45.

MCC § 2-25-090(a) (emphasis added).

81. A violation of Illinois’s PIPA “constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.” 815 ILCS 530/20.

82. Thus, a violation of PIPA is also a violation of the Ordinance.

83. Equifax has violated Section 10 of PIPA by failing to notify Chicago residents that a breach of the security of its system data had occurred in the most expedient time possible and without unreasonable delay.

84. Because of this delay, Chicago residents with compromised Personal Information have been unable to adequately protect themselves from potential identity theft.

85. Equifax has also violated PIPA by failing to provide disclosure notifications to Chicago residents, as required by Section 10 of PIPA.

86. Equifax's violations of PIPA constitute unlawful practices under the Illinois Consumer Fraud and Deceptive Business Practices Act and, accordingly, violate the Ordinance.

87. The penalty for violating the Ordinance is a fine of not less than \$2,000.00 nor more than \$10,000.00 for each offense. MCC § 2-25-090(f). Moreover, "[e]ach day that a violation continues shall constitute a separate and distinct offense to which a separate fine shall apply." *Id.*

88. A violation of the Ordinance also entitles the City to equitable relief, including, but not limited to, restitution. MCC § 2-25-090(e)(4).

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

- A. find that Equifax has violated the Ordinance by failing to notify Chicago residents that a breach of the security of its system data had occurred in the most expedient time possible and without unreasonable delay, and by failing to provide disclosure notifications to Chicago residents, as required by Section 10 of PIPA;
- B. fine Equifax for each failure to properly provide such notification to a Chicago resident, in the amount of \$10,000 for each day the violation has existed and continues to exist, and grant the City equitable relief, including, but not limited to, restitution, pursuant to the Ordinance; and
- C. grant any other relief that this Court deems appropriate.

## **COUNT II**

### **Deceptive Practice – Failure to Safeguard Personal Information – Violation of § 2-25-090**

89. Chicago realleges and incorporates herein by reference each of the foregoing allegations contained this Complaint as though fully alleged in this Count.

90. The Ordinance provides that any "unlawful practice" under the Illinois Consumer Fraud and Deceptive Business Practices Act constitutes a violation of the Ordinance.

91. Section 2 of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/2, provides:

Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in section 2 of the 'Uniform Deceptive Trade Practices Act', approved August 5, 1965, in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby. In construing this section consideration should be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5 (a) of the Federal Trade Commission Act.

92. While engaging in trade or commerce, Equifax has engaged in conduct that constitutes a deceptive act or practice declared unlawful under Section 2 of the Illinois Consumer Fraud and Deceptive Business Practices Act, in that it made deceptive public representations and communications about the nature of its data security safeguards to the public, including Chicago residents, assuring them that their Personal Information was safe.

93. Equifax intended that the public, including Chicago residents, rely on its deceptive representations and communications regarding the security of Personal Information.

94. Rather than following industry best practices to keep Personal Information protected, secure, and not susceptible to access by unauthorized third parties, Equifax instead handled that Personal Information in such a manner that it was compromised.

95. Equifax's conduct constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act and, accordingly, violates the Ordinance.

96. The penalty for violating the Ordinance is a fine of not less than \$2,000.00 nor more than \$10,000.00 for each offense. MCC § 2-25-090(f). Moreover, "[e]ach day that a violation continues shall constitute a separate and distinct offense to which a separate fine shall apply." *Id.*

97. A violation of the Ordinance also entitles the City to equitable relief, including, but not limited to, restitution. MCC § 2-25-090(e)(4).

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

- A. find that Equifax has violated the Ordinance by engaging in conduct that constitutes a deceptive act or practice declared unlawful under Section 2 of the Illinois Consumer Fraud and Deceptive Business Practices Act;
- B. fine Equifax for each violation involving a Chicago resident, in the amount of \$10,000 for each day the violation has existed and continues to exist, and grant the City equitable relief, including, but not limited to, restitution, pursuant to the Ordinance; and
- C. grant any other relief that this Court deems appropriate.

### COUNT III

#### **Unfair Practice – Failure to Safeguard Personal Information – Violation of § 2-25-090**

98. Chicago realleges and incorporates herein by reference each of the foregoing allegations contained this Complaint as though fully alleged in this Count.

99. While conducting trade or commerce, Equifax has engaged in conduct that constitutes an unfair act or practice declared unlawful under Section 2 of the Illinois Consumer Fraud and Deceptive Business Practices Act, in that it failed to implement procedures and practices to prevent unauthorized access to its data systems and the Personal Information of Chicago residents.

100. Equifax's unique role as a credit-reporting firm made the need for it to keep Personal Information secure especially acute.

101. Equifax was aware of the risks associated with identity theft. On its website, Equifax lists "some of the ways identity theft might happen," including when identity thieves "steal electronic records through a data breach."

102. Equifax ignored known, foreseeable threats of unauthorized access to its data systems, including by failing to heed warnings from security experts about the vulnerabilities in the Apache Struts framework, and by failing to encrypt sensitive Personal Information.

103. Rather than following industry best practices to keep Personal Information protected, secure, and not susceptible to access by unauthorized third parties, Equifax instead handled that Personal Information in such a manner that it was compromised.

104. Equifax's conduct constitutes an unfair practice deemed unlawful under the Consumer Fraud and Deceptive Business Practices Act and, accordingly, violates the Ordinance.

105. The penalty for violating the Ordinance is a fine of not less than \$2,000.00 nor more than \$10,000.00 for each offense. MCC § 2-25-090(f). Moreover, "[e]ach day that a violation continues shall constitute a separate and distinct offense to which a separate fine shall apply." *Id.*

106. A violation of the Ordinance also entitles the City to equitable relief, including, but not limited to, restitution. MCC § 2-25-090(e)(4).

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

- A. find that Equifax has violated the Ordinance by engaging in conduct that constitutes an unfair act or practice declared unlawful under Section 2 of the Illinois Consumer Fraud and Deceptive Business Practices Act;
- B. fine Equifax for each violation involving a Chicago resident, in the amount of \$10,000 for each day the violation has existed and continues to exist, and grant the City equitable relief, including, but not limited to, restitution, pursuant to the Ordinance; and
- C. grant any other relief that this Court deems appropriate.

#### COUNT IV

##### **Deceptive Practice – Equifax Required Consumers to Waive Legal Rights and Misrepresented its Credit Monitoring Services as “Free” – Violation of § 2-25-090**

107. Chicago realleges and incorporates herein by reference each of the foregoing allegations contained this Complaint, as though fully alleged in this Count.

108. While engaging in trade or commerce, Equifax has engaged in conduct that constitutes a deceptive act or practice declared unlawful under Section 2 of the Illinois Consumer Fraud and Deceptive Business Practices Act, in that it made deceptive public representations by initially falsely representing to residents of Chicago, and all others, that it was offering “complimentary identity theft protection and credit file monitoring.”

109. In fact, enrollment for this service required the public, including Chicago residents, to sign an agreement which included a broad class action waiver and individual arbitration agreement, and was subject to automatic renewal for a fee after one year. Thus, it was not complimentary and employed deception and coercion in an unconscionable effort to bind affected persons to arbitrate their claims, and otherwise limit their legal rights.

110. Equifax intended that the public, including Chicago residents, rely on its deceptive representations and communications regarding the nature of its services and intended that people would, among other things, agree to binding individual arbitration of their claims and to automatic renewal of a fee-based service after one year.

111. Equifax’s conduct constitutes a deceptive practice deemed unlawful under the Consumer Fraud and Deceptive Business Practices Act and, accordingly, violates the Ordinance.

112. The penalty for violating the Ordinance is a fine of not less than \$2,000.00 nor more than \$10,000.00 for each offense. MCC § 2-25-090(f). Moreover, “[e]ach day that a

violation continues shall constitute a separate and distinct offense to which a separate fine shall apply.” *Id.*

113. A violation of the Ordinance also entitles the City to equitable relief, including, but not limited to, restitution. MCC § 2-25-090(e)(4).

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

- A. find that Equifax has violated the Ordinance by engaging in conduct that constitutes a deceptive act or practice declared unlawful under Section 2 of the Illinois Consumer Fraud and Deceptive Business Practices Act;
- B. fine Equifax for each violation involving a Chicago resident, in the amount of \$10,000 for each day the violation has existed and continues to exist, and grant the City equitable relief, including, but not limited to, restitution, pursuant to the Ordinance; and
- C. grant any other relief that this Court deems appropriate.

#### **COUNT V**

#### **DECLARATORY AND INJUNCTIVE RELIEF**

114. Chicago realleges and incorporates herein by reference each of the foregoing allegations contained this Complaint, as though fully alleged in this Count.

115. Pursuant to 735 ILCS 5/2-701, this Court “may make binding declarations of rights, having the force of final judgments . . . including the determination . . . of the construction of any statute, municipal ordinance, or other governmental regulation . . . and a declaration of the rights of the parties interested.”

116. Such a declaration of rights “may be obtained . . . as incident to or part of a complaint . . . seeking other relief as well.” 735 ILCS 5/2-701(b).

117. Chicago seeks a judgment declaring that Equifax has violated the Ordinance.

118. Chicago further contends that Equifax’s data security measures were inadequate to protect the public’s sensitive personal information.



119. Upon information and belief, these data security measures remain inadequate. Chicago residents will continue to suffer or be vulnerable to injury, unless this is rectified through injunctive relief.

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

- A. declare that Equifax has violated the Ordinance;
- B. issue a preliminary and permanent injunction requiring Equifax to use adequate security measures to protect its websites and computer systems from attacks by hackers and to prevent future unauthorized access of Chicago residents' sensitive personal and financial information; and
- C. grant any other relief that this Court deems appropriate

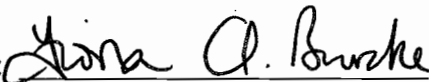
**REQUEST FOR JURY TRIAL**

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

Dated: September 28, 2017

Respectfully submitted,

EDWARD N. SISKEL  
Corporation Counsel, City of Chicago

BY:   
Attorney

Attorney No. 90909  
John L. Hendricks, Deputy Corporation Counsel  
Thomas P. McNulty, Senior Counsel  
Ellen W. McLaughlin, Assistant Corporation Counsel  
Jordan A. Rosen, Assistant Corporation Counsel  
Constitutional and Commercial Litigation Division  
City of Chicago Department of Law  
30 N LaSalle St., Suite 1230  
Chicago, IL 60602  
312-744-6975, 742-0307, 742-5147, 744-9018  
John.Hendricks@cityofchicago.org  
Thomas.McNulty@cityofchicago.org  
Ellen.McLaughlin@cityofchicago.org  
Jordan.Rosen@cityofchicago.org

Diane M. Pezanoski, Deputy Corporation Counsel  
Fiona A. Burke, Chief Assistant Corporation Counsel  
Michael C. Zumwalt, Assistant Corporation Counsel  
Aviation, Environmental, Regulatory, and Contracts Division  
City of Chicago Department of Law  
30 N. LaSalle St., Suite 1400  
Chicago, IL 60602  
312-744-6996, 744-6929, 744-5218  
Diane.Pezanoski@cityofchicago.org  
Fiona.Burke@cityofchicago.org  
Michael.Zumwalt@cityofchicago.org