UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF GEORGIA

ATLANTA DIVISION

LAURA BRODER, individually and on behalf of herself and other similarly situated, Plaintiff v. EQUIFAX, INC., Defendant	Case No. **COMPLAINT - CLASS ACTION** JURY TRIAL DEMANDED

Plaintiff Laura Broder, on behalf of herself and all others similarly situated, hereby alleges the following, based on personal knowledge as to herself and on information and belief based on the investigation of counsel, and public sources as to all other matters:

I. NATURE OF THE ACTION

1. Plaintiff brings this class action for damages, injunctive relief, and other relief pursuant to state privacy and tort laws related to an unprecedented data breach.

2. Defendant Equifax, Inc. ("Equifax") is a leading provider of identity and credit monitoring services to hundreds of millions of consumers. In addition to those services, Equifax contracts with third parties such as banks, insurance

companies, and governmental entities to perform identity verification, and other services that make Equifax a guardian of personally-identifiable data. Through both its direct relationships with its clients, and through its third party contracting business, Equifax has obtained highly confidential, sensitive financial and other data concerning hundreds of millions of consumers around the world.

3. Equifax's business model is to monetize this data by providing it as requested by its clients pursuant to its agreement with them and also by selling access to this confidential and sensitive information to banks, insurance companies and other third parties. In short, the services offered by Equifax give it responsibility for personal and private information for maintaining the confidentiality of hundreds of millions of consumers, most of whom have no choice in the matter. It is no exaggeration to say that Equifax is thus a significant guardian of the public trust, and that it plays a key role in the complex financial and security systems that keep citizens and consumers safe in the United States and abroad.

4. The action arises out of the disturbing security breach that released to hackers of as yet undisclosed origin personal information—including social security numbers, drivers' license numbers, addresses, credit card data and verifying security information —of 143 million U.S. citizens. This is almost half of

the population of the United States. These consumers may be further victims of identity theft, unauthorized access to their most important online accounts, and will require years of ongoing monitoring and remediation.

5. On September 7, 2017, Equifax first informed the public that hackers had accessed Equifax's online databases and mined personal information. Personal information such as addresses, birth dates, social security numbers, drivers' license information, credit card information, and online security password information has been jeopardized. Critically, Equifax admitted that it has been aware of the breach since July 29, 2017. As of the date of the filing of this complaint, however, Equifax has not affirmatively and definitively notified any or all specific individuals that their personal data has been compromised. This failure to warn its clients and consumers, or to provide remediation to the extent possible, is indefensible.

6. Rather than protect those whose data had been entrusted to it (including Equifax's own clients), Equifax has focused its resources on protecting itself. Equifax has not notified anyone privately and specifically about the extent of the breach. Instead, before Equifax notified consumers of the breach, it was furiously lobbying Congress to pass legislation that would grant Equifax immunity from serious liability. Indeed, even *after* Equifax announced its breach,

the Company sought to profit from it directly, by advising consumers who were simply trying to determine if their data was at issue to buy a new Equifax product, an identify protection product which cost an additional $19.95 per month. Moreover, Equifax attempted to insert a class action waiver and arbitration agreement, seeking to bind inquiring and concerned consumers to limited remedies.

7. Equifax's actions are unlawful and unconscionable. This complaint seeks remedies for the harmed individuals.

II. JURISDICTION AND VENUE

8. This Court has jurisdiction over this action under 28 U.S.C. § 1332(a)(1) because Plaintiff and Defendant are citizens of different states and the amount in controversy exceeds the sum or value of $75,000, exclusive of interest and costs. This Court also has jurisdiction under 28 U.S.C. § 1332(d) because it is brought as a class action, at least one member of the proposed class is a citizen of a different state from the Defendant, and the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs.

9. Venue is proper in this District under 28 U.S.C. § 1391(a) because the Defendant resides here and because a substantial part of the events or omissions giving rise to the claim occurred here.

III. PARTIES

10. Plaintiff Laura Broder is a resident of Eastchester, New York. Plaintiff Broder discovered that she was likely affected by the data breach by entering information on Equifax's website. Plaintiff Broder is at elevated risk of identity theft and loss due to Equifax's actions, and has spent time and effort seeking to remedy the harm caused by Equifax.

11. Defendant Equifax, Inc. ("Equifax" or the "Company") is an international corporation with its principal place of business in Atlanta, Georgia.

12. Equifax is a leading provider of consumer information services. Equifax provides what it calls "data analytics" for more than 500 million consumers and 81 million businesses worldwide. Equifax offers services related to identity authentication and management, fraud prevention, privacy, and data security.

13. Equifax offers these services outright, and contracts with hundreds of other businesses (including insurance companies) to provide identity authentication.

IV. FACTS GIVING RISE TO THE CLAIMS

Equifax's Role as Guardian of Sensitive Personal and Financial Data

14. Equifax is in the business of accessing, storing, and monetizing personal and private consumer information. In so doing, Equifax has taken on an

enormous responsibility to its clients, who are entrusting information used for financial and security purposes, including but not limited to Social Security numbers, as well as consumers whose data Equifax receives through its third-party contracts.

15. Equifax cultivates the trust of its clients, promising on its website services that will allow consumers to "Be In Control" and maintain "Peace of Mind." Equifax also contracts with financial institutions, insurance companies, and other businesses to provide and store consumers' private and personal information for decisions on lending, identity verification, and other services. Since its founding in 1899, and through the solicitations associated with these services, Equifax has amassed and maintains repositories of personal and financial data relating to hundreds of millions of consumers collected for over many years. Its contracts with third party banks and insurance companies similarly promise confidentiality and security.

16. Notwithstanding the heavy weight of public trust Equifax solicited, on September 7, 2017, Equifax disclosed that it had discovered that from mid-May until July 29, 2017, hackers accessed people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers from databases that Equifax maintains. Equifax also disclosed that credit card numbers were

stolen for about 209,000 people, and dispute documents with personal identifying information for about 182,000 people. Equifax has not identified the time period for which the data was accessed; the nationality or location of the individuals who are affected; what credit card companies are involved; what state driver's license are affected; and – critically – what steps consumers should take to prevent identify theft, other than paying Equifax to protect the information that Equifax already promised it was protecting.

17. Inexplicably, Equifax waited six weeks to inform the public of this unprecedented breach of trust. Equifax discovered the breach on July 29, but took no action to inform consumers for six weeks. Even now, a general announcement that consumers "may" be affected is inadequate, particularly when prophylactic measures cost money and time. In its failure to be specific as to who Equifax at least knows is affected. Equifax creates a giant externality, shifting the burden of curing the harm to the entire public. The public must now fend for itself.

18. Victims of this breach will require long-term monitoring. Not only was personal and private information for over a hundred Americans disclosed, but also information that consumers use to safeguard their online accounts. Equifax has admitted that certain security questions and answers used on some websites to verify users' identity may also have been exposed. Having that

information in hand would allow hackers to change their targets' passwords and other account settings.

19. According to one online security expert, the fact "[t]hat the intruders were able to access such a large amount of sensitive consumer data via a vulnerability in the company's Web site suggests Equifax may have fallen behind in applying security updates to its Internet-facing Web applications."

20. The scope of the breach is currently unknown. Equifax has stated that it "engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted."

Equifax Fails to Remedy Its Breach

21. Following the breach, in a plot twist that might have been dreamed up by Joseph Heller (author of *Catch-22*), Equifax invited concerned and inquiring consumers to sign up on its website for Equifax's "TrustedID Premier" credit monitoring service. Equifax offered TrustedID service free for a year, at a cost of $19.95. This Equifax product was obviously already plainly inadequate to protect consumers' identity, because of course Equifax had disclosed that massive amounts of data had already been improperly accessed. Moreover, a year of future "protection" does not cure the past data breach. Hackers have downloaded untold

amounts of data from Equifax's website, and that information will certainly not expire in a year. This did not stop Equifax from seeking to extract additional money from people who were concerned that Equifax's breach might have affected them.

22. As one expert has observed, "credit monitoring services typically only look for new account fraud and do little or nothing to prevent fraud on existing consumer credit accounts." Accordingly, the remedy offered by Equifax is inadequate. "Credit monitoring services rarely prevent identity thieves from stealing your identity. The most you can hope for from these services is that they will alert you as soon as someone does steal your identity." As one expert in online security has stated, "[t]he fact that the breached entity (Equifax) is offering to sign consumers up for its own identity protection services strikes me as pretty rich."

23. Equifax has offered no refund to subscribers, who have paid monthly fees yet were informed about the data breach via press release. "[Q] Can you help me cancel my existing Equifax credit monitoring subscription/service? [A] If you have an existing subscription to an Equifax credit monitoring product, you may elect to cancel your existing subscription and enroll in TrustedID Premier. To do so, you will need to log into your current product and proceed with the

cancellation process, which can be found in the Manage Billing portion of your online account."

24. Similarly, Equifax has offered no meaningful remedy to individuals whose data it has come to possess through no act of their own. Equifax has admitted that it has compromised the privacy of data it obtained from unidentified business partners: "[Q] I've never signed up for Equifax services, why do you have my information? [A] As a nationwide consumer reporting agency, Equifax receives information from a variety of businesses and other sources."

Equifax Fails to Take Responsibility

25. Equifax has not accepted responsibility for the enormous amount of data it has collected. Quite the opposite. Equifax wants to both profit from its "data analytics," whereby Equifax is paid to collect and synthesize personal and private information, and immunize itself from legal accountability.

26. Equifax has attempted to strip legal rights from those who were affected by the breach. When the breach was first reported, Equifax operated a website that would inform consumers if they were affected by the disclosure—*if* these consumers waived the right to participate in a class action and agreed to arbitration. Equifax has since stated that "[i]n response to consumer inquiries, we have made it clear that the arbitration clause and class action waiver included in

the Equifax and TrustedID Premier terms of use does not apply to this cybersecurity incident."

27. Less than a week after announcing the U.S. security breach, moreover, Equifax announced a separate breach in Argentina, that apparently resulted from Equifax's use, on its web application there, on a username/password combination of admin/admin to gain access.

28. As law professor Eric Chaffee told CNN last week: "It's pretty remarkable how long Equifax has been aware of the problem and did not disclose it. The main problem here is the failure to disclose a catastrophic cyberattack that compromised the information that is at the heart of Equifax's business model. This created a duty to disclose this attack in a timely fashion to investors, potential investors, and those whose data was compromised."

29. Rather than address its failure to secure consumer's data, Equifax has instead spent its money on lobbying for immunity for mishandling personal and private information. Equifax reported $500,000 in lobbying records through the first half of this year on issues relating to data security, breach notification, "data breach response" and "cybersecurity threat information sharing." Indeed, just hours before Equifax announced the U.S. data breach – but weeks after Equifax

learned of it -- the House Financial Services Committee was debating proposed amendments to the Fair Credit Reporting Act for which Equifax had lobbied.

V. CLASS ALLEGATIONS

30. Plaintiff brings this action on behalf of herself and classes of those similarly situated, defined as follows:

a) **Subscription Class**: All persons who, as of September 7, 2017, purchased subscription services from Equifax related to identify protection or credit monitoring services ("Subscription Services").

b) **Identity Class**: All persons whose personal and financial information was contained in or on the Equifax database and whose personal and financial information was stolen or otherwise misappropriated as a result of the Data Breach that was announced on or about September 7, 2017.

Excluded from the Classes are Defendants; officers, directors, and employees of Defendants; any entity in which Defendants have a controlling interest; the affiliates, legal representatives, attorneys, heirs, and assigns of the Defendants.

31. Plaintiff is a member of the Identity Class.

32. The conduct of Defendant has caused injury to members of the Classes.

33. The members of the Classes are so numerous that joinder of all members is impracticable, as approximately 143 million individuals' personal and financial information may have been compromised.

34. The members of the Classes are readily ascertainable. Indeed, members of the Classes can easily be identified by records maintained by Defendant. Notice can be provided by means permissible under the Federal Rules of Civil Procedure.

35. There are substantial questions of law and fact common to the Classes. These questions include, but are not limited to, the following:

a) Whether Equifax failed to provide adequate security and or protection for its computer systems containing Plaintiff's and members of the potential Classes' financial and personal data;

b) Whether Equifax's conduct resulted in the unauthorized breach of its computer systems containing Plaintiff's and members of the potential Classes' financial and personal data;

c) Whether Equifax unfairly charged Plaintiff and members of the potential Subscription Class for services that had little or no value;

d) Whether Equifax disclosed (or directly or indirectly caused to be disclosed) private financial and personal information of Plaintiff and members of the potential Classes;

e) Whether Equifax owed a legal duty to Plaintiff and members of the potential Classes to use reasonable care regarding their personal information;

f) Whether Equifax unreasonably delayed in announcing this breach;

g) Whether Equifax's attempt to strip potential members of the Classes of their rights to sue in court and participate in a class action are enforceable;

h) Whether Equifax breached its duties to exercise reasonable due care in obtaining, using, retaining, and safeguarding Plaintiff's and members of the potential Classes' personal and financial information;

i) Whether Equifax was negligent;

j) Whether Equifax's breach of its duties proximately caused damages to Plaintiff and the other members of the Classes;

k) Whether Equifax has breached its duty to maintain the privacy of Plaintiffs' information;

l) Whether Plaintiff and members of the Classes have suffered damages, including an increased risk of identity theft as a result of Equifax's failure to protect Plaintiff's and the members of the Classes' personal and financial information; and

m) Whether Plaintiff and other members of the Classes are entitled to compensation, damages, and/or other relief as a result of the breach of duties alleged herein.

36. Plaintiff's claims are typical of the claims of all members of the Classes. The same events and conduct that give rise to Plaintiff's claims and legal theories also give rise to the claims and legal theories of the Classes. Specifically, Plaintiff's and members of the Classes' claims arise from Equifax's failure to install and maintain reasonable security measures to protect Plaintiff's and members of the Classes' personal and financial information.

37. Equifax has acted and refused to act on grounds generally applicable to the Classes described herein.

38. Prosecuting separate actions by individual members of the Classes would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Equifax.

39. Plaintiff will fairly and adequately represent the interests of the Classes. There are no disabling conflicts of interest between Plaintiff and the Classes.

40. Plaintiff is represented by experienced counsel who are qualified to litigate this case. The lawsuit will be capably and vigorously pursued by Plaintiff and her counsel.

41. A class action is superior to other available methods for a fair and efficient adjudication of this controversy since joinder of all members of the Classes is impracticable.

42. The damages suffered by individual members of the Classes may be relatively small in comparison with the expense and burden associated with individual litigation, which make it impossible for them to individually redress the harm done to them.

43. Proceeding as a class action will permit an efficient administration of the claims of members of the Classes. Class treatment of these claims will save time, ensure uniformity in factual and legal rulings, and allows all parties to conserve legal fees that would otherwise be expended in litigating common issues piecemeal.

VI. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

Negligence

44. Plaintiff restates and realleges the foregoing allegations as if fully set forth herein.

45. Equifax had a duty to exercise reasonable care to protect and secure Plaintiff's and the members of the Classes' personal and financial information within its possession or control from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This highly confidential personal and financial information includes but is not limited to full legal names, birth dates, Social Security numbers, street addresses, email addresses, employment information, and income data, and other personal information.

46. Equifax's duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiff's and the members of the Classes' personal and financial information in their possession was adequately secured and protected, and was retained only for legitimate purposes and with adequate storage, retention and disposal policies.

47. Equifax further had a duty to implement processes that would detect a breach of its security systems in a timely manner.

48. In light of the special relationship between Plaintiff and members of the Classes and Equifax, whereby Equifax required Plaintiff and members of the Classes to provide highly sensitive confidential personal and financial information as a condition of application, availability of health insurance, and employment, Equifax undertook a duty of care to ensure the security of such information.

49. Through its acts or omissions, Equifax breached its duty to use reasonable care to protect and secure Plaintiff's and the members of the Classes' personal and financial information within its possession or control. Equifax breached its duty by failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and members of the Classes' personal and financial information, failing to adequately monitor the security of its network allowing unauthorized access to Plaintiff's and the members of the Classes' personal and financial information, and failing to recognize in a timely manner that Plaintiff's and members of the Classes' personal and financial information had been compromised.

50. But for Equifax's wrongful and negligent breach of the duties owed to Plaintiff and the members of the Classes, the Data Breach would not have occurred and Plaintiff's and the members of the Classes' personal and financial information would not have been compromised.

51. The injury and harm suffered by Plaintiff and the members of the Classes was the reasonably foreseeable and probable result of Equifax's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the members of the Classes' personal and financial information in its possession or control. Equifax knew or should have known that its systems and technologies for processing and securing Plaintiff's and members of the Classes' personal and financial information had significant vulnerabilities.

52. As a result of Equifax's negligence, Plaintiff and the members of the Classes have incurred damages, and are at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse.

SECOND CLAIM FOR RELIEF

Invasion of Privacy

53. Plaintiff restates and realleges the foregoing allegations as if fully set forth herein.

54. Plaintiff had a reasonable expectation of privacy in the personal and financial information Defendant mishandled.

55. By failing to keep Plaintiff's personal and financial information safe, and by making Plaintiff's personal information vulnerable to hackers, Defendant invaded Plaintiff's privacy by intruding into Plaintiff's private affairs in a manner

that would be highly offensive to a reasonable person; publicizing private facts about Plaintiff, which is highly offensive to a reasonable person; using and appropriating Plaintiff's identity without Plaintiff's consent; and violating Plaintiff's right to privacy, through the improper use of Plaintiff's personal and financial information properly obtained for a specific purpose for another purpose, or the disclosure to a third party.

56. Defendant invaded Plaintiff's right to privacy and intruded into Plaintiff's private affairs by misusing and/or disclosing Plaintiff's personal and financial information without her informed, voluntary, affirmative, and clear consent.

57. Defendant's misuse and disclosures of personal information have frustrated Plaintiff's reasonable expectations of privacy in her personal and financial information.

THIRD CLAIM FOR RELIEF

Violation of the Fair Credit Reporting Act ("FCRA")

58. Plaintiff restates and realleges the foregoing allegations as if fully set forth herein.

59. Plaintiff and members of the Classes are consumers for purposes of FCRA, 15 U.S.C. § 1681a(c).

60. Under FCRA, a "consumer reporting agency" is "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." 15 U.S.C. § 1681a(f).

61. Equifax is a "consumer reporting agency" because, for a fee, Equifax provides credit and other financial information about consumers for the purpose of creating credit reports.

62. Under FCRA, Equifax is required to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

63. The private and personal data maintained by Equifax, and disclosed by the data breach, is covered by FCRA because it has "bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1).

64. Under FCRA, the circumstances under which Equifax may provide a consumer report are enumerated by 15 U.S.C. § 1681b. None of these purposes allow Equifax to release data as occurred in the data breach.

65. Equifax provided credit reports by disclosing Plaintiff and members of the Classes' private personal information. Equifax willfully, or recklessly, violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. These decisions by Equifax were willful because Equifax allowed its technology and security measures to lag through the deterioration of its policies and procedures.

66. Plaintiff and members of the Classes have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiffs and each of the Nationwide Class members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

67. Plaintiffs and the Nationwide Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2) & (3).

FOURTH CLAIM FOR RELIEF

Violation of N.Y. Gen. Bus. Law § 349

68. Plaintiff restates and realleges the foregoing allegations as if fully set forth herein.

69. Defendant negligently and recklessly failed to provide reasonable and adequate security measures. Defendant also unreasonably delayed—and continues to delay—informing Plaintiff and members of the Classes about the Data Breach and disclosure of Plaintiff and members of the Classes' personal and financial information after Equifax knew that the Data Breach had occurred.

70. Equifax violated N.Y. Gen. Bus. Law § 349 by failing to properly implement adequate, commercially reasonable security measures to protect Plaintiff and members of the Classes' private information. Equifax ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measure to prevent, detect, and mitigate the security breach. Then, Equifax failed to take reasonable steps to correct and remedy the breach, including failing to inform those who had been impacted by the breach. Defendant Equifax saved money by not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the security breach. Defendant Equifax's failure to

implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff and members of the Classes that is not offset by countervailing benefits to consumers or competition or reasonable avoidable by consumers.

71. Defendant Equifax's failure to take preventative and corrective steps to protect private information entrusted to it offends public policy and is unjust, oppressive, and unscrupulous, and causes substantial injury to consumers.

72. Plaintiff and members of the Classes have suffered actual damages including improper disclosure of their private information, lost value of their private information, lost time and money incurred to mitigate and remediate the effects of the Security Breach, payment for services that had reduced value, including the increased risk of identity theft that resulted and continues to face them.

73. Equifax's unlawful conduct was consumer-oriented in that it was designed to, had the capacity to, and did, deceive consumers and affect consumer decisions in the State of New York.

74. Equifax's conduct described herein affected the public interest, and in particular, the public interest in New York State, because that conduct injured consumers in New York.

75. Plaintiffs' and members of the Classes' injuries were proximately caused by Defendant's violations of the N.Y. Gen. Bus. Law § 349, which was conducted with reckless indifference toward the rights of others, such that an award of punitive and/or treble damages is warranted.

FIFTH CLAIM FOR RELIEF

Violation of Georgia Fair Business Practices Act, O.C.G.A. § 10-1-390, *et seq*.

76. Plaintiff restates and realleges the foregoing allegations as if fully set forth herein.

77. The acts and omissions alleged herein affect trade and commerce pursuant to O.C.G.A. § 10-1-392(28).

78. Equifax's acts and omissions principally occurred, or were directed from, its headquarters and offices in the state of Georgia. Equifax's actions in obtaining Plaintiffs' personal and private information, and failures to secure the same, were directed from Georgia.

79. Equifax was entrusted with Plaintiffs' personal and private information.

80. Equifax engaged in unfair or deceptive acts or practices in the in violation of the Fair Business Practices Act, as follows:

a) Equifax failed to maintain privacy and data protection sufficient to safeguard Plaintiff and members of the Classes' personal and private information;

b) Equifax obtained and stored personal and private data, and accepted fees from its business partners to do the same, without sufficient protections;

c) Equifax did not disclose to consumers that it was entrusted with any particular consumer's data, or that its computer systems and data security practices could not protect the data; and

d) Equifax failed to accurately or fully disclose the breach, and unreasonably delayed in making the breach public.

81. Equifax knew or should have known that its computer systems and data security practices did not safeguard the Plaintiff's and members of the Classes' personal, private information; could not deter hackers; and could not detect and remedy a security breach.

82. Plaintiff and members of the Classes suffered damages from the foregoing breaches of duty.

83. Plaintiffs and members of the Classes are entitled to damages as well as injunctive relief, including, but not limited to:

a) Full disclosure of the extent of the data breach;

b) Remedial action for Plaintiff and members of the Classes, including credit-monitoring and other credit services;

c) Implementation of policies and procures that will eliminate or substantially reduce the likelihood of future data breaches;

d) Implementation of technology, such as encryption of data, that will reduce the impact of any future data breach;

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays:

A. That the Court determine that this action may be maintained as a class action under Rule 23(a) and (b)(3) of the Federal Rules of Civil Procedure and direct that reasonable notice of this action, as provided by Rule 23(c)(2) of the Federal Rules of Civil Procedure, be given to members of the Classes;

B. Monetary damages in excess of $5,000,000, including disgorgement of fees for Subscription Services;

C. Injunctive relief, including but not limited to the provision of credit monitoring services for a period of at least twenty-five years, the provision of bank monitoring services for a period of at least twenty-five years, the provision of credit restoration services for a period of at least twenty-five

years, and the provision of identity theft insurance for a period of at least twenty-five years;

D. That the Court award Plaintiff and the Classes attorneys' fees and costs, including expert and consultant fees, as well as pre-judgment and post-judgment interest as permitted by law; and

E. F. That the Court award Plaintiff and the Classes such other and further relief as may be deemed necessary and appropriate.

VIII. JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(c), Plaintiff demands a trial by jury on all matters so triable.

Dated: September 15, 2017

SIMMONS HANLY CONROY LLC

By: */s/ David F. Miceli*

David F. Miceli, GA #503900
One Court Street
Alton, IL 62002
- and -
P.O. Box 2519
Carrolton, GA 30112
Telephone: 618.259.2222
Facsimile: 618.259.2251
dmiceli@simmonsfirm.com

Lesley A. Weaver (SBN 191305)
Matthew S. Weiler (SBN 236052)
Emily C. Aldridge (SBN 299236)
BLEICHMAR FONTI & AULD LLP
1999 Harrison Street, Suite 670
Oakland, California 94612
Telephone: 415.445.4003
Facsimile: 415.445.4020
E-mail: lweaver@bfalaw.com
E-mail: mweiler@bfalaw.com
E-mail: ealdridge@bfalaw.com

Jayne Conroy
Andrea Bierstein
SIMMONS HANLY CONROY LLC
112 Madison Avenue
New York, New York 10016-7416
Telephone: 212.784.6400
Facsimile: 212.213.5949
E-mail: jconroy@simmonsfirm.com
E-mail: abierstein@simmonsfirm.com