IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

Summit Credit Union, individually and on behalf of a class of similarly situated credit unions, Plaintiff, v. Equifax Inc., Defendant.	**COMPLAINT** JURY TRIAL DEMANDED CIVIL ACTION NO: _____

Plaintiff Summit Credit Union ("Summit"), by and through its undersigned counsel, individually and on behalf of a class of similarly situated credit unions, files this Class Action Complaint against Defendant Equifax, Inc. ("Equifax"), and states the following:

INTRODUCTION

1. This litigation stems from the largest data breach in history of a financial services industry gatekeeper charged with one primary task: collecting and maintaining consumers' most sensitive personal and financial information.

2. That company—Equifax—utterly failed at this task, allowing hackers to breach the gates and gain unfettered access to the sensitive information of millions. In so doing, Equifax set off a chain reaction that threatens the trustworthiness and stability of the financial system for individuals and institutions alike.

3. Equifax is one of the largest consumer credit reporting agencies in the United States. Equifax gathers, analyzes, and maintains credit-reporting information on over 820 million individual consumers and over 91 million businesses.

4. On September 7, 2017, Equifax announced that hackers had exploited a vulnerability in Equifax's U.S. website to illegally gain access to consumer files.[1]

5. Equifax must now be held accountable for its failures and for a cybersecurity incident so massive that it could prove detrimental to overall American economic growth.

PARTIES

6. Plaintiff Summit Credit Union (Summit) is a State of Wisconsin chartered credit union with its principal place of business at

[1] Equifax, *Cybersecurity Incident & Important Consumer Information* (Sept. 8, 2017), https://www.equifaxsecurity2017.com/.

4800 American Parkway, Madison, Wisconsin. Summit was officially chartered in 1935. It has $2.6 billion in assets, operates 34 locations throughout the State of Wisconsin, and has over 162,000 members. It is regulated by the National Credit Union Administration (NCUA) as a federally insured, state-chartered credit union.

7. Defendant Equifax, Inc. is a publicly traded corporation with its principal place of business at 1550 Peachtree Street NE, Atlanta, Georgia.

JURISDICTION AND VENUE

8. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d). At least one class member (Plaintiff, Summit Credit Union) is of diverse citizenship from Defendants, there are more than 100 class members, and the aggregate amount in controversy exceeds $5 million, before interest and costs.

9. This Court may exercise personal jurisdiction over Equifax because Equifax has sufficient minimum contacts in Georgia. Specifically, Equifax's principal place of business is in Georgia, and Equifax regularly conducts business throughout the state, including advertising and selling products and services within Georgia.

10. Venue is proper in this District and division under 28 U.S.C. § 1391(a) because Equifax's principal place of business is in Georgia, and a substantial part of Equifax's acts and omissions giving rise to the allegations in this Complaint occurred in this District.

FACTUAL ALLEGATIONS

Background

11. Equifax is one of the largest consumer credit reporting agencies in the United States, and it is the oldest of the three major U.S. credit-reporting agencies. Equifax has over $3 billion in annual revenue, and its common stock is traded on the New York Stock Exchange.

12. Equifax gathers and maintains credit-reporting information on over 820 million individual consumers and over 91 million businesses.

13. For consumer files, Equifax collects a substantial amount of sensitive personal information. Equifax's consumer credit files include individuals' names, current and past addresses, birth dates, social security numbers, and telephone numbers; credit account information, including the institution name, type of account, date the account was opened, payment history, credit limit, and balance; credit inquiry information, including credit applications; and public-record information, including liens, judgments, and bankruptcy filings.

14. Equifax analyzes the information that it collects and generates consumer credit reports, which it sells to businesses like retailers, insurance companies, utility companies, banks and financial institutions, and government agencies.

15. Equifax also provides services to consumers, including credit monitoring and identity-theft-protection products. Additionally, Equifax is required by law to provide one free annual credit report to consumers.

16. Equifax has an obligation to consumers to use every reasonable measure to protect the sensitive consumer information that it collects from exposure to hackers and identity thieves.

Equifax Data Breach

17. From mid-May to late July of 2017, hackers exploited a vulnerability in Equifax's U.S. web server software to illegally gain access to certain consumer files. Investigators believe that the point of entry may have been a software application called Apache Struts.[2]

18. The potential vulnerability of the Apache Strut software was no secret. Security researchers with Cisco Systems Inc. warned in March

[2] AnnaMaria Androtis *et al.*, *Equifax Hack Leaves Consumers, Financial Firms Scrambling*, WALL STREET JOURNAL, Sept. 8, 2017, *available at* https://www.wsj.com/articles/equifax-hack-leaves-consumers-financial-firms-scrambling-1504906993

2017 that a flaw in the Apache Struts software was being exploited in a "high number" of cyber attacks. Despite this warning, Equifax continued to use the software. And Equifax was reportedly using an outdated version of Apache Struts at the time of the data breach.[3]

19. Over this nearly three-month period, the Equifax hackers accessed consumer names, social security numbers, birth dates, addresses, and driver's license numbers. The compromised data contains complete profiles of consumers whose personal information was collected and maintained by Equifax.

20. Equifax estimates that 143 million Americans were impacted by this breach, although it admits that it is still in the process of "conducting a comprehensive forensic review" with a cybersecurity firm "to determine the scope of the intrusion."[4]

21. In addition to accessing sensitive personal information, the hackers also accessed an estimated 209,000 consumer credit card numbers, and an estimated 182,000 dispute records containing additional personal information were compromised. [5]

---

[3] *Id.*

[4] Equifax, *Cybersecurity Incident & Important Consumer Information* (Sept. 8, 2017), https://www.equifaxsecurity2017.com/.

[5] *Id.*

22. Equifax reportedly discovered this breach on July 29, 2017.[6]

23. After Equifax discovered this breach but before Equifax disclosed the breach to the public, three high-level executives sold shares in the company worth nearly $1.8 million.[7] On August 1, just three days after Equifax discovered the breach, Equifax Chief Financial Officer John Gamble sold $946,374 worth of stock, and President of U.S. Information Solutions Joseph Loughran exercised options to sell $584,099 worth of stock. The next day, President of Workforce Solutions, Rodolfo Ploder, sold $250,458 worth of stock.

24. Equifax did not report this breach to the public until September 7, 2017. Equifax has not explained its delay in reporting this breach to the public.

25. Since the breach was publicly revealed, federal regulators have said that they are examining Equifax's actions. The FBI is also investigating the breach, and two congressional committees announced that they would hold hearings.[8]

---

[6] *Id.*

[7] Anders Melin, *Three Equifax Managers Sold Stock Before Cyber Hack Revealed*, BLOOMBERG (Sept. 7, 2017), *available at* https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack.

[8] Androtis, *supra*.

26. Upon information and belief, although six weeks have passed since Equifax discovered the breach, the investigation is still ongoing, and the identity of the hackers is still unknown.

27. This breach is one of the largest data breaches in history, due to both the number of people exposed and the sensitivity of the information compromised. As reported by the Wall Street Journal, "[t]he Equifax hack is potentially the most dangerous of all, though, because the attackers were able to gain vast quantities of personal identification—names, addresses, Social Security numbers and dates of birth—at one time."[9]

28. The Equifax breach is unique because many consumers may not be aware that their personal information was compromised. Equifax obtains its credit reporting information from banks, credit card issuers, retailers, lenders, and public records. Accordingly, many consumers are not aware that Equifax or other reporting companies are collecting or retaining their sensitive personal information.

[9] *Id.*

Consumers and Financial Institutions Are Harmed by the Breach

29. Initial reports indicate that hackers accessed credit card information of over 200,000 U.S. consumers in this breach. Identity thieves can use these numbers to make fake credit cards, which can then be sold or used to make unauthorized purchases that are then charged to a member's[10] or customer's account.

30. Additionally, sensitive personal and financial information like the information compromised in this breach is extremely valuable to thieves and hackers. These criminals have gained access to complete profiles of individuals' personal and financial information. They can then use these data sets to steal the identities of the consumers whose information has been compromised or sell it to others who plan to do so. The identity thieves can assume these consumers' identities (or create entirely new identities from scratch) to make transactions or purchases, open credit or bank accounts, apply for loans, forge checks, commit immigration fraud, obtain a driver's license in the member's or customer's name, obtain government benefits, or file a fraudulent tax return.

[10] Credit unions are wholly owned by their members and provide financial services to those members.

31. When identity thieves fraudulently use a victim's personal information, the victim frequently suffers financial consequences. A 2014 Department of Justice report on identity theft reported that 65% of identity theft victims experienced direct or indirect financial losses. In addition to the damage caused to consumers, credit unions and banks ultimately bear significant additional losses, as they typically indemnify their customers or members for fraudulent charges.

32. When sensitive personal information is compromised, consumers must exercise constant vigilance on their financial and personal records to ensure that fraudulent activity has not occurred. Consumers are forced to spend additional time monitoring their credit and finances as well as dealing with any potentially fraudulent activity. In turn, the banks and credit unions where these consumers bank must do the same.

33. Consumers also face significant emotional distress after theft of their identity. The fear of financial harm can cause significant stress and anxiety for many consumers. According to the Department of Justice, an estimated 36% of identity theft victims experienced moderate or

severe emotional distress as a result of the crime.[11] This stress can also impact financial institutions, which are forced to expend additional customer service resources helping their stressed customers. Customers experiencing severe anxiety related to identity theft are often hesitant to use some banking services altogether, instead opting to use cash. As a result, financial institutions forgo many of the transaction fees, ATM fees, interest, or other charges that they may have otherwise collected on these accounts.

34. Financial institutions—both those used by legitimate consumers and those used by identity thieves—also feel the financial impact of identity theft.

35. When credit or debit card information is compromised, issuers face significant costs in cancelling and reissuing those payment cards to members or customers. Cancelling the compromised card numbers and reissuing new credit cards to their members or customers is the only way financial institutions can ensure accounts are not charged for unauthorized purchases. Some consumers even change or close their

[11] *Id.*

accounts in the wake of the fraud, resulting in additional cost and lost profits to the financial institution.

36. Moreover, financial institutions like Summit are responsible for any fraudulent activity on their members' accounts. When fraudulent charges are made to members' or customers' existing (legitimate) accounts, financial institutions largely bear the cost of indemnifying these charges. For instance, when a member reports fraudulent activity on a credit or debit card, Summit must credit back to its member the amount of any fraudulent charge. Yet Summit has no recourse to recover the charge against the retailer or merchant where the fraudulent purchase was made.

37. Financial institutions face even larger costs associated with entirely new accounts created by identity thieves. With the complete data sets that hackers have now acquired from the Equifax breach, criminals can use these stolen identities or create a new identity from scratch. They can then use this identity to apply for new lines of credit, loans, or other accounts with financial institutions.

38. Financial institutions are responsible for *all* charges to these fraudulently opened accounts. The losses associated with these newly opened accounts only increase over time. When complete consumer

profiles have been compromised, financial institutions experience continuous losses as identity thieves move on from one consumer profile to the next. With a breach of this magnitude, there is virtually no limit to the amount of fraudulent account openings financial institutions may face.

39. These risks are very real in the wake of the Equifax breach. These financial institutions and their members' or customers' information has been compromised as part of the Equifax breach. Because of this breach, for example, Summit Credit Union's pre-approval offers for auto-recapture loans, student loan offers, and auto and credit card pre-approvals may have been compromised.

40. As a result, financial institutions face considerable costs associated with monitoring, preventing, and responding to fraudulent charges and account openings. Financial institutions must implement additional fraud monitoring and protection measures, investigate potentially fraudulent activity, and indemnify members or customers for fraudulent charges. Financial institutions will also need to take other necessary steps to protect themselves and their members or customers, including notifying members or customers, as appropriate, that their

accounts may have been compromised. These burdens impact credit unions, who frequently serve individual and small business customers.

41. Financial institutions will also face increased regulatory compliance costs going forward as a result of this incident. Federal regulators have already begun considering the implications of the breach and are likely to implement additional requirements to protect consumers from the financial risks associated with this breach. For example, additional reports and plans will likely be required to satisfy regulators. Financial institutions will be required to directly bear the costs of these additional measures.

42. Financial institutions are also concerned about the chilling effect this breach may have on future lending as consumers deal with the impact of the breach on their finances and credit, as well as on their emotional wellbeing. Customers or members are often without access to their accounts for several days at a time while credit or debit cards are replaced or accounts are changed. Additionally, some customers are hesitant to use card transactions altogether in the wake of a major breach. This results in lost fees and interest to the financial institutions issuing these cards.

43. Equifax had a duty to properly secure its website from hackers, to use available technology to encrypt and otherwise secure consumers' personal information using industry standard methods, and to act reasonably to prevent the foreseeable harm to Plaintiff and the Class, which it knew would result from a data breach.

44. Indeed, Equifax's role as a credit-reporting firm made the need for it to secure the information it held especially acute. And that role has itself created an additional burden for financial institutions, who have typically relied on the files at credit-reporting agencies like Equifax to determine whether applications for consumer credit or loans are creditworthy. Not only has that process now been thrown into jeopardy for Summit and the financial institutions it seeks to represent, but also such financial institutions are now without a vital source of verifying consumers' identities due to the extent of the personal and financial information compromised by the Equifax breach.[12]

[12] *See* Telis Demos, *Equifax Hack Could Slow Down Fast Loans*, WALL STREET JOURNAL (Sept. 11, 2017), *available at* https://www.wsj.com/articles/equifax-hack-could-slow-down-fast-loans-1505147969.

45. For all of these reasons, the breach has sent shockwaves throughout the entire financial services industry, and its reverberations will be felt for years to come.

The Breach was the Result of Equifax's Failure to Properly and Adequately Secure its U.S. Website

46. The Equifax breach was the direct result of Equifax's failure to properly and adequately secure its U.S. website.

47. Specifically, Equifax failed to heed warnings from security experts about the vulnerabilities in its Apache Strut software. Additionally, Equifax failed to update this software to its latest version.

48. Equifax admitted in public statements that hackers were able to access this data by exploiting a vulnerability in Equifax's U.S. website application to illegally gain access to consumer files.

49. Equifax should have recognized and identified the flaws in its data security and should have taken measures to fix these vulnerabilities. Equifax had a duty to take advantage of what experts had already learned about security vulnerabilities and to use industry best practices, such as updating software to the latest version, to prevent a security breach.

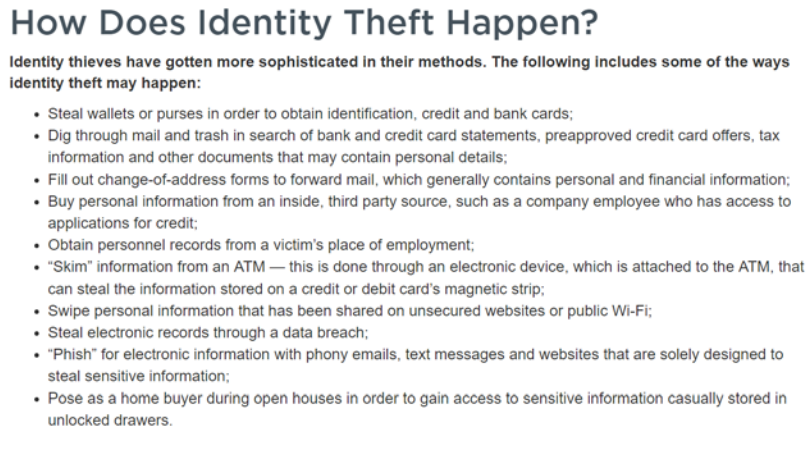
50. Even before this incident, Equifax was on notice of potential problems with its web security. A security researcher has reported that in

August, hackers claimed to have illegally obtained credit-card information from Equifax, which they were attempting to sell in an online database.[13] Equifax had a duty to respond to a report of a significant software security flaw. Despite Equifax's knowledge of these potential security threats, Equifax willfully (or at least negligently) failed to enact appropriate measures to ensure the security of its consumer files, including failing to encrypt sensitive personal and financial consumer information.

51. The harm to consumers and financial institutions as a result of Equifax's failure to adequately secure its computer systems and websites was therefore foreseeable to Equifax.

52. Equifax is well aware of the costs and 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."

[13] Androtis, *supra*.; *See also,* Thomas Fox-Brewster, *A Brief History of Equifax Security Fails,* FORBES, Sept. 8, 2017, available at: https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#63dc4270677c.



How Does Identity Theft Happen?

Identity thieves have gotten more sophisticated in their methods. The following includes some of the ways identity theft may happen:

- Steal wallets or purses in order to obtain identification, credit and bank cards;
- Dig through mail and trash in search of bank and credit card statements, preapproved credit card offers, tax information and other documents that may contain personal details;
- Fill out change-of-address forms to forward mail, which generally contains personal and financial information;
- Buy personal information from an inside, third party source, such as a company employee who has access to applications for credit;
- Obtain personnel records from a victim's place of employment;
- "Skim" information from an ATM — this is done through an electronic device, which is attached to the ATM, that can steal the information stored on a credit or debit card's magnetic strip;
- Swipe personal information that has been shared on unsecured websites or public Wi-Fi;
- Steal electronic records through a data breach;
- "Phish" for electronic information with phony emails, text messages and websites that are solely designed to steal sensitive information;
- Pose as a home buyer during open houses in order to gain access to sensitive information casually stored in unlocked drawers.

14

53. In fact, Equifax has published a report on the "Emotional Toll of Identity Theft." In its report, Equifax states that "identity theft victims may experience similar emotional effects as victims of violent crimes, ranging from anxiety to emotional volatility." The report also cites a survey finding that "69 percent felt fear for personal financial security; 50 percent of respondents said they had feelings of powerlessness or helplessness; and 29 percent said they felt shame or embarrassment."[15]

54. Financial institutions are on the front lines following a data breach, working with these consumers when identity theft does occur,

---

[14] Equifax, *How Does Identity Theft Happen?*, https://www.equifax.com/personal/education/identity-theft/how-does-identity-theft-happen (last accessed September 10, 2017).

[15] Equifax, *A Lasting Impact: The Emotional Toll of Identity Theft*, Feb. 2015, *available at* https://www.equifax.com/assets/PSOL/15-9814_psol_emotionalToll_wp.pdf.

increasing the cost to financial institutions, including credit unions, whose customer bases are usually comprised of individuals and small businesses.

55. Because Equifax is aware of the negative consequences of identity theft, Equifax also offers products aimed at protecting consumers from identity theft. For example, Equifax advertises its "Equifax Complete™ Premier Plan" as "Our Most Comprehensive Credit Monitoring and Identity Protection Product."[16] The product promises to alert consumers of changes to their credit score and credit report provide text message alerts to changes, lock the consumer's credit file by unapproved third parties, and automatically scan suspicious websites for consumers' personal information.

56. Equifax was aware of the risk posed by its insecure and vulnerable website. It was also aware of the extraordinarily sensitive nature of the personal information that it maintains as well as the resulting impact that a breach would have on consumers and financial institutions—including Plaintiff and the other class members.

---

[16] Equifax, *Equifax Complete ™ Premier Plan: Our Most Comprehensive Credit Monitoring and Identity Protection Product*, https://www.equifax.com/personal/products/credit/monitoring-and-reports (last accessed Sept. 10, 2017).

Equifax Had a Duty to Prevent and Timely Report this Breach

57. Equifax had a duty to prevent breach of consumers' sensitive personal information.

58. Following several high-profile data breaches in recent years, including Target, Home Depot, Yahoo, and Sony, Equifax was on notice of the very real risk that hackers could exploit vulnerabilities in its data security. Moreover, Equifax has considerable resources to devote to ensuring adequate data security.

59. Nonetheless, Equifax failed to invest in adequate cyber security measures to properly secure its U.S. website from the threat of hackers.

60. Consumers and financial institutions were harmed not only by the breach itself but also by Equifax's failure to timely report this breach to the public.

61. Equifax discovered this breach on July 29, 2017, but did not report it to the public until nearly six weeks later on September 7, 2017.

62. According to the Wall Street Journal, an anonymous source familiar with the investigation states that "Equifax executives decided to hold off on informing the public until they had more clarity on the number of people affected and the types of information that were

compromised."[17] But Equifax has not yet given an official explanation for its delay in reporting this breach to the public. In the time between when Equifax discovered this breach and when it reported the breach to the public, however, three of its top executives were able to sell—and sold—substantial sums of stock in the company, presumably avoiding the financial losses associated with the negative press Equifax has received since the breach.[18]

63. Because of this delay, consumers with compromised personal information and credit card information have been unable to adequately protect themselves from potential identity theft for several weeks.

64. Financial institutions have also been unable to alert their members or customers of the risk in a timely manner, or to implement measures to detect and prevent potential fraud in the time before the breach was disclosed.

---

[17] Androtis, *supra*.

[18] Equifax's stock prices dropped almost 15% the day after the breach was publicly announced—the largest decline in nearly two decades. Ben Eisen, *Equifax Shares on Pace for Worst Day in 18 Years*, WALL STREET JOURNAL (Sept. 8, 2017), *available at* https://blogs.wsj.com/moneybeat/2017/09/08/equifax-shares-on-pace-for-worst-day-in-18-years/.

65. This resulted in additional harm to Plaintiff, the Class, and consumers that they would not have suffered if Equifax had not delayed in reporting the breach to the public.

CLASS ACTION ALLEGATIONS

66. Plaintiff Summit Credit Union brings this action on behalf of itself and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), and (b)(3), on behalf of the following class:

> Credit unions in the United States (including its Territories and the District of Columbia) that issue payment cards or perform, facilitate, or support other banking products and services, whose customers' and members' personal information was collected or amassed by Equifax and compromised in the 2017 breach of Equifax's U.S. website (the "CU Class").

67. Plaintiff is a member of the CU Class, as defined above.

68. The members of the CU Class are readily ascertainable, and Equifax likely has access to addresses and other contact information that may be used for providing notice to CU Class members.

69. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of its claims on a class-wide basis using the same evidence as would be used in individual actions alleging the same claims.

70. This action has been brought and may be properly maintained on behalf of the class proposed herein under Federal Rule of Civil Procedure 23 and satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of its provisions.

Class Certification Requirements

71. *Numerosity: Federal Rule of Civil Procedure 23(a)(1).* The CU Class members are so numerous and geographically dispersed that individual joinder of all class members is impracticable. As of the first quarter of 2017, in the United States, there were 5,737 credit unions with more than 100 million members, with 1.34 trillion in assets. [19]The Court and all parties will benefit substantially from a single lawsuit that addresses all of the class members' claims in this case. Class members will be easily identifiable from publicly-available records, such as NCUA records of federal and state chartered credit unions. Class members may be notified of this action by recognized, court-approved methods of dissemination, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

[19] 2015 Statistical Report, World Council of Credit Unions (Sept. 11, 2017). http://www.woccu.org/impact/global_reach/statreport.

72. *Commonality and Predominance: Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).* Common questions of law and fact in this case predominate over questions affecting individual CU Class members. Common factual and legal questions include, but are not limited to:

(a) whether Equifax failed to provide adequate security and/or protection on its websites that contained sensitive consumer information;

(b) whether Equifax's conduct resulted in the breach of its U.S. website and the exposure of consumers' sensitive information;

(c) whether Equifax notified the public of this breach in a timely manner;

(d) whether Equifax failed to encrypt sensitive consumer information;

(e) whether Equifax's actions were negligent;

(f) whether Equifax owed a duty to Plaintiff and the Class;

(g) whether the harm to Plaintiff and the Class was foreseeable;

(h) whether Plaintiff and the Class are entitled to injunctive relief; and

(i) whether Plaintiff and the Class are entitled to damages, and the amount of such damages.

73. *Typicality: Federal Rule of Civil Procedure 23(a)(3).* Plaintiff's claims are typical of the other CU Class members' claims because all class members were comparably injured through Equifax's negligence as described in detail above. All credit unions will face the same costs

associated with this breach, as described above. The factual bases of these claims are common to all class members.

74. *Adequacy: Federal Rule of Civil Procedure 23(a)(4).* Plaintiff Summit is an adequate class representative because its interests do not conflict with the interests of the other members of the CU Class it seeks to represent. Plaintiff Summit has retained counsel who are competent and experienced in complex class action litigation. Moreover, Plaintiff Summit intends to prosecute this action vigorously. Plaintiff Summit and its counsel will fairly and adequately protect the class's interests in this case.

75. *Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2).* Equifax has acted or refused to act on grounds generally applicable to Plaintiff Summit and the other members of the class. Accordingly, final injunctive relief and declaratory relief, as described below, is appropriate with respect to the CU Class as a whole.

76. *Superiority: Federal Rule of Civil Procedure 23(b)(3).* A class action is superior to any other available means for the fair and efficient adjudication of this case. No unusual difficulties are likely to arise in the management of this class action. The damages that Plaintiff and the other class members suffered are relatively small compared to the burden and expense required to litigate their claims individually. Accordingly, it

would be impracticable for class members to seek redress individually from Equifax.

77. Even if CU Class members could afford the relatively high cost of individual litigation, the court system could not. Individual litigation creates the potential for inconsistent or contradictory judgments. It also increases the delay and expense to all parties and the court system. By comparison, a class action presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

78. Moreover, separate individual actions create the risk of different courts imposing different and incompatible standards of conduct on Equifax. This creates needless duplication and prolonged proceedings, and is inappropriate because common legal and factual questions predominate over individual questions.

CAUSES OF ACTION

Count I
Negligence

79. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

80. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care and diligence in obtaining, processing, and retaining

Plaintiff's members' sensitive personal information and credit card numbers.

81. Defendant owed a duty to Plaintiff and the Class to adequately secure consumers' personal and financial information.

82. Defendant breached this duty by: (1) failing to properly secure its U.S. website from intrusion by a third party; (2) allowing a third party to exploit a vulnerability in this website and access consumers' sensitive personal and financial information; (3) failing to detect this breach for several weeks; and (4) failing to notify consumers of this breach for nearly six weeks.

83. Defendant knew or should have known of the risks associate with potential vulnerabilities in its websites and computer systems.

84. Defendant knew or should have known that its failure to take reasonable measures to secure these websites and computer systems against obvious risks would result in harm to Plaintiff and the Class.

85. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered substantial damages. Upon information and belief, these damages include, but are not limited to, the cost of cancelling and reissuing credit cards to members or customers of Plaintiff and the Class, changing or closing member or customer

accounts, notifying members or customers that their accounts may have been compromised, implementing additional fraud monitoring and protection measures, investigating potentially fraudulent activity, indemnifying members or customers for fraudulent charges, unwinding or absorbing charges to fraudulently-opened new credit accounts of varying kinds, complying with additional regulatory requirements imposed as a result of the breach, and taking other necessary steps to protect themselves and their members or customers. Upon information and belief, Plaintiff and the Class also lost profits as a result of their members or customers being unwilling or unable to use their credit cards following the breach.

Count II
Negligence *Per Se*

86. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

87. Equifax's failure to adequately safeguard consumers' sensitive personal information and credit cards numbers from data breach constitutes negligence *per se* because this conduct violates Section 5 of the Federal Trade Commission ("FTC") Act.[20]

[20] 15 U.S.C. §§ 41 *et seq*.

88. The FTC Act exists to "prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."

89. The FTC has interpreted Section 5 of the FTC Act to include the unfair practice of failing to maintain reasonable security for members' or customers' sensitive or personal information.

90. As part of its duties under the FTC Act, the FTC "has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information."[21]

91. Accordingly, Equifax violated Section 5 of the FTC Act by failing to use reasonable security measures to adequately protect its consumers' sensitive personal information.

92. Plaintiff and the Class are within the group of persons Section 5 of the FTC Act was designed to protect, because Plaintiff and the Class are responsible for indemnifying members or customers for

[21] Federal Trade Commission, *Enforcing Privacy Promises*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (last accessed Sept. 10, 2017).

fraudulent charges. Additionally, some Class members (including Plaintiff) are credit unions, which are organized as cooperatives whose members are consumers.

93. As a direct and proximate result of Defendant's violation of Section 5 of the FTC Act, Plaintiff and the Class have suffered substantial damages. Upon information and belief, these damages include, but are not limited to, the cost of cancelling and reissuing credit cards to members or customers of Plaintiff and the Class, changing or closing member or customer accounts, notifying members or customers that their accounts may have been compromised, implementing additional fraud monitoring and protection measures, investigating potentially fraudulent activity, indemnifying members or customers for fraudulent charges, unwinding or absorbing charges to fraudulently-opened accounts, complying with additional regulatory requirements imposed as a result of the breach, and taking other necessary steps to protect themselves and their members or customers. Upon information and belief, Plaintiff and the Class also lost profits because their members or customers were unwilling or unable to use their credit cards following the breach.

Count III
Negligent Misrepresentation by Omission

94. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

95. Through collecting, analyzing, and maintaining sensitive consumer information, Equifax represented to Plaintiff and the Class that it maintained adequate data security measures, and that the data security measures it employed were adequate to protect the sensitive consumer financial information maintained in its computer system.

96. Defendant knew or should have known that its data security measures were not, in fact, adequate to protect the sensitive consumer financial information maintained in its computer system.

97. Defendant failed to disclose vulnerabilities in its website and computer system that made its sensitive consumer information susceptible to breach.

98. Defendant was required to disclose this fact to Plaintiff, the Class, and consumers.

99. Defendant also failed to timely discover the breach, and failed to timely disclose the breach to Plaintiff, the Class, and consumers once Defendant had discovered it.

100. Had Plaintiff, the Class, and consumers been aware of the vulnerabilities in Defendant's websites and computer systems, leaving sensitive consumer information susceptible to breach, Plaintiff, the Class, and consumers would have taken action to prevent this data from being breached or required Equifax to take immediate action to resolve these weaknesses.

101. As a direct and proximate result of Defendant's negligent misrepresentation by omission, Plaintiff and the Class have suffered substantial damages. Upon information and belief, these damages include, but are not limited to, the cost of cancelling and reissuing credit cards to members or customers of Plaintiff and the Class, changing or closing member or customer accounts, notifying members or customers that their accounts may have been compromised, implementing additional fraud monitoring and protection measures, investigating potentially fraudulent activity, indemnifying members or customers for fraudulent charges, charges to fraudulently-opened accounts, complying with additional regulatory requirements imposed as a result of the breach, and taking other necessary steps to protect themselves and their members or customers. Upon information and belief, Plaintiff and the

Class also lost profits because of their members or customers being unwilling or unable to use their credit cards following the breach.

Count IV
Declaratory and Injunctive Relief

102. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

103. Plaintiff and the Class are entitled to a declaratory judgment under the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq*. The Declaratory Judgment Act authorizes this Court to enter a declaratory judgment stating the rights and legal relations of the parties and grant further relief if necessary. Additionally, the Court has authority to enjoin tortious acts or acts in violation of federal or state statute.

104. Plaintiff and the Class contend that Equifax's data security measures were inadequate to protect consumers' sensitive personal information. Upon information and belief, these data security measures remain inadequate. Plaintiff and the Class will continue to suffer injury unless this is rectified.

105. Plaintiff and the Class seek a declaratory judgment stating that Equifax owed and continues to owe a duty to adequately and appropriately secure consumers' sensitive personal and financial information, and that Equifax has a duty to timely disclose to the public

any breach of that data; that Equifax breached and continues to breach this duty by failing to adequately secure its websites and computer systems containing members' or customers' sensitive personal and financial information; Equifax's breach of this duty caused the data breach which occurred between mid-May and late-June of 2017; and Plaintiff and the Class were forced to incur the costs of cancelling and reissuing credit cards to members or customers of Plaintiff and the Class, changing or closing member or customer accounts, notifying members or customers that their accounts may have been compromised, implementing additional fraud monitoring and protection measures, investigating potentially fraudulent activity, indemnifying members or customers for fraudulent charges, charges to fraudulently-opened accounts, complying with additional regulatory requirements imposed as a result of the breach, and taking other necessary steps to protect themselves and their members or customers.

106. Plaintiff and the Class also seek corresponding injunctive relief 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 consumers' sensitive personal and financial information.

107. If injunctive relief is not granted, Plaintiff and the Class will suffer irreparable injury and will not have an adequate legal remedy in the event of future data breaches. Many of the injuries resulting from these breaches are not easily quantifiable, and Plaintiff and the Class will be forced to bring multiple additional lawsuits.

108. The burden to Plaintiff and the Class if this Court issues an injunction is far greater than the burden to Equifax if the Court does not do so. The cost of improving data security and applying reasonable measures to protect consumer data should be minimal, particularly given the nature of Equifax's business and its considerable financial resources. Equifax *already* has a duty to provide these protections. If future data breaches occur, though, upon information and belief, Plaintiff and the Class will suffer further financial losses associated with cancelling and reissuing credit cards to members or customers of Plaintiff and the Class, changing or closing member or customer accounts, notifying members or customers that their accounts may have been compromised, implementing additional fraud monitoring and protection measures, investigating potentially fraudulent activity, indemnifying members or customers for fraudulent charges, charges to fraudulently-opened accounts, complying with additional regulatory requirements imposed as

a result of the breach, and taking other necessary steps to protect themselves and their members or customers.

109. Such an injunction would benefit the public by decreasing the risk of future Equifax data breaches, eliminating potential future injuries that would result from another breach.

110. Plaintiff and Class members, therefore, request the injunctive and declaratory relief detailed above.

RELIEF REQUESTED

Plaintiff, individually and on behalf of the Class, respectfully requests that the Court enter judgment in its favor and against Equifax Inc. as follows:

A. Certification of the proposed class, including appointment of Plaintiff's counsel as class counsel;

B. An order temporarily and permanently enjoining Equifax from the negligent business practices alleged in this Complaint;

C. Costs, restitution, damages, and disgorgement in an amount to be determined at trial;

D. Other damages as permitted by applicable laws;

E. Pre- and post-judgment interest on any amounts awarded;

F. Costs and attorneys' fees; and

G. Such other or further relief as may be appropriate.

September 11, 2017

Robins Kaplan LLP

By: _____*/s/ James Kitces*_____

Stacey P. Slaughter (MN #0296971)
William H. Stanhope (GA #675025)
James Kitces (GA#424420)
Sam E. Khoroosi (MN # 0397190)

800 LaSalle Avenue
Suite 2800
Minneapolis, MN 55402
T: 612 349 8500
F: 612 339 4181
sslaughter@robinskaplan.com
wstanhope@robinskaplan.com
jkitces@robinskaplan.com
skhoroosi@robinskaplan.com

Susan Brown
Michael Ram
2440 West El Camino Real
Suite 100
Mountain View, CA 94040
T: 650.784.4007
sbrown@robinskaplan.com
mram@robinskaplan.com

Turke & Strauss LLP
Mary C. Turke
Samuel J. Strauss
613 Williamson Street, Suite 201
Madison, WI 53703
T: 608 237 1775
F: 608 509 4423
mary@turkestrauss.com
sam@turkestrauss.com

Attorneys for Plaintiff Summit Credit Union