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

SUNCOAST CREDIT UNION, individually and on behalf of all other similarly situated financial institutions, **Plaintiff** **v.** **EQUIFAX, INC.,** **Defendant**	**Case No.** **COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Suncoast Credit Union ("Suncoast"), by its undersigned counsel, upon personal knowledge as to itself and its own acts, and upon information and belief as to all other matters, respectfully brings this putative class action, individually and on behalf of all other similarly situated financial institutions, against Equifax Inc. ("Equifax"), alleging as follows:

INTRODUCTION

1. Plaintiff Suncoast, individually and on behalf of similarly situated financial institutions (including, without limitation, credit unions, banks, community banks, and other financial institutions (the "Class" (defined below)),

brings this class action on behalf of financial institutions that suffered, and continue to suffer, financial losses and increased data security risks that directly result from Equifax's egregious failure to safeguard, and affirmative mishandling of, financial institutions' customers' (i) highly sensitive, personally identifiable information, including, without limitation, names, Social Security numbers, birth dates, addresses, and driver's license numbers (collectively, "PII"), and (ii) payment card data, including, without limitation, credit and debit card numbers, primary account numbers ("PANs"), card verification value numbers ("CVVs"), expiration dates, and zip codes (collectively, "Payment Card Data").

2. Between at least May 2017 and July 2017, Equifax was subject to one of the largest data breaches in this country's history when data thieves gained access to the highly sensitive PII of over 145.5 million U.S. consumers – roughly 44% of the United States population – as well as the Payment Card Data for an untold number of credit and debit cards issued by Suncoast and other financial institutions (the "Equifax Data Breach," "Data Breach," or "Breach").

3. Despite the fact that the threat of a data breach was a well-known risk to Equifax, as it acknowledged in its corporate filings, Equifax failed to take reasonable steps to adequately protect and affirmatively mishandled the only product that it exclusively trades and is responsible for protecting: the ultra-sensitive, highly-sought-after PII, Payment Card Data, and financial information of

millions of individuals. Suncoast and the Class are now left to deal with the direct consequences of Equifax's failures and active misfeasance.

4. Equifax's CEO admitted: "The company failed to prevent sensitive information from falling into the hands of wrongdoers. . . . [T]he breach occurred because of both human error and technology failures." *See* Oversight of the Equifax Data Breach: Answers for Consumers, Hearing before the U.S. House Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection (Oct. 3, 2017) (Prepared Testimony of Richard F. Smith), https://democrats-energycommerce.house.gov/ committee-activity/hearings/hearing-on-oversight-of-the-equifax-data-breach- answers-for-consumers ("Smith Testimony").

5. The Data Breach was the inevitable result of Equifax's longstanding lax approach to the security of PII and Payment Card Data, an approach characterized by its actions, inaction, neglect, incompetence, and an overarching desire to minimize costs. Equifax's data security deficiencies were so significant that even after hackers entered its systems, their activities went undetected for at least two months—despite red flags that should have caused Equifax to discover their presence and thwart, or at least minimize, the damage.

6. Equifax's actions left highly sensitive PII and Payment Card Data exposed and accessible to hackers for months. Consequently, Suncoast has

incurred, and will continue to incur, significant damages in connection with, among other things, cancelling and replacing customers' credit and debit cards, covering fraudulent purchases, closing fraudulent bank and credit accounts, responding to credit disputes, taking protective measures to reduce risk of identity theft and loan fraud, and assuming financial responsibility for various types of fraudulent activity related to stolen identities and misuse of PII and Payment Card Data.

7. The financial harms caused by Equifax's negligent handling of PII and Payment Card Data have been, and will continue to be, borne in large part by financial institutions—such as Suncoast—that issue payment cards, process and hold various loans and credit products, process and hold various deposit accounts, and service accounts held by individuals whose PII and Payment Card Data was compromised by the Breach. Such harms include, without limitation, canceling and reissuing an untold number of compromised credit and debit cards, reimbursing customers for fraudulent charges, closing fraudulent bank and credit accounts, responding to credit disputes resulting from fraudulent accounts being opened as a result of compromised customer data, increasing fraudulent activity, including the implementation of alternative customer authentication methods, monitoring, taking appropriate action to mitigate the risk of identity theft and fraudulent loans and other banking activity, sustaining reputational harm, and notifying customers of potential fraudulent activity.

8. Suncoast seeks to recover the damages and costs that it and other similarly situated financial institutions have been forced to bear as a direct result of the Equifax Data Breach. Suncoast also seeks to obtain appropriate equitable relief to mitigate future harm that is certain to occur in light of the unprecedented scope of this Breach.

PARTIES

9. Plaintiff Suncoast Credit Union is a Florida-chartered credit union with its principal place of business at 6801 East Hillsborough Avenue, Tampa, FL 33610.

10. Defendant Equifax Inc. is a publicly traded corporation with its principal place of business at 1550 Peachtree Street NE, Atlanta, GA 30309.

JURISDICTION AND VENUE

11. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d). The value of the aggregated claims of the individual Class members exceed $5,000,000 exclusive of interest and costs, there are more than 100 putative Class members, and diversity exists because Suncoast and the majority of the putative Class members are citizens of a different state than Equifax.

12. This Court has personal jurisdiction over Equifax because Equifax maintains its principal headquarters in this District, Equifax is registered to

conduct business in Georgia, including this District, Equifax regularly conducts business in Georgia, including this District, and Equifax has sufficient minimum contacts in Georgia, including this District. Equifax intentionally avails itself of this jurisdiction by conducting its corporate operations here, and promoting, selling, and marketing Equifax products and services to resident Georgia consumers and entities, including consumers and entities in this District.

13. Venue is proper in this District, under 28 U.S.C. §1391(a), because Equifax's principal place of business is in this district, and a substantial part of the events, acts, and omissions giving rise to Suncoast's claims (*i.e.*, the Data Breach) occurred in this District.

FACTS

I. Background.

14. Equifax is the oldest and second-largest consumer credit reporting agency in the United States. Equifax was founded in 1899 and had $3.1 billion in revenue in 2016. Its common stock is traded on the New York Stock Exchange under the ticker symbol "EFX."

15. Equifax's 2016 Form 10-K states that it:

> [I]s a leading global provider of information solutions and human resources business process outsourcing services for businesses, governments and consumers. We have a large and diversified group of clients, including financial institutions, corporations, governments and individuals. Our products and services are based on comprehensive

> databases of consumer and business information derived from numerous sources, including credit, financial assets, telecommunications and utility payments, employment, income, demographic and marketing data. We use advanced statistical techniques and proprietary software tools to analyze all available data, creating customized insights, decision-making solutions and processing services for our clients.

See https://investor.equifax.com/~/media/Files/E/Equifax-IR/documents/financial-information/form-10-k.pdf (last accessed Oct. 3, 2017).

16. Equifax gathers and maintains credit-reporting information on over 820 million individual consumers and over 91 million businesses. Equifax gets its data from companies that have extended credit to consumers in the past, currently extend credit to consumers, or who wish to extend credit to consumers. Credit card companies, banks, credit unions, retailers, and auto and mortgage lenders all report the details of consumer credit activity to Equifax. *See How Do Credit Reporting Agencies Get Their Information?* (July 2, 2014), https://blog.equifax.com/credit/how-do-credit-reporting-agencies-get-their- information/.

17. In addition, Equifax obtains PII and Payment Card Data directly from consumers who purchase credit reporting, monitoring, and other products from Equifax. Equifax collects a substantial and diverse amount of sensitive personal information about consumers, including (i) individuals' names, current and past addresses, birth dates, Social Security numbers, and telephone numbers; (ii) credit account information, including the institution name, type of account held, date an

account was opened, payment history, credit limit, and balance; (iii) credit inquiry information, including credit applications; and (iv) public-record information, including liens, judgments, and bankruptcy filings.

18. Armed with this data, Equifax sells four primary data products: credit services, decision analytics, marketing, and consumer assistance services:

a. Credit services. Equifax generates consumer credit reports. When lending institutions, such as Suncoast, review a request for credit, they purchase a consumer credit report from Equifax to assist in making decisions about whether credit should be extended and in what amount.

b. Decision Analytics. Equifax packages detailed transaction histories with analytics about the ways an individual interacts with certain debt. Credit issuers pay more for these reports because they offer a deeper analysis of the appropriateness of certain credit for certain consumers.

c. Marketing. Credit issuers that offer pre-approved credit pay a marketing fee to Equifax for a list of consumers who meet predetermined requirements. This information is used to extend offers of credit to consumers who meet an institution's desired criteria.

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

19. Much like a bailment of personal property, the receipt by Equifax of uniquely-identifying consumer credit-reporting information, PII, and Payment Card Data for Equifax's own business purposes places Equifax in a special relationship with consumers, Suncoast, and the Class members, which rely on Equifax to maintain the security (and hence, the uniquely-identifying nature) of such information. The resulting harm to Suncoast from mishandling the security and confidentiality of this information was, at all times, foreseeable by Equifax.

20. Equifax had, and continues to have, a well-established and clear legal duty to act reasonably to protect the sensitive information that it collects and possesses from exposure to hackers and identity thieves. *See*, *e.g.*, Fair Credit Reporting Act, 15 U.S.C. §1681(a)(4) and (b).

II. Suncoast relied on Equifax to adequately protect its customers' PII and Payment Card Data.

21. When Suncoast and Class members provide Equifax with their customers' PII and Payment Card Data, or when Equifax comes by such information in some other manner, Suncoast reasonably expects Equifax to store such information in a safe and confidential manner, using all reasonable safeguards and protections. The potential harm from doing otherwise is obvious to Equifax, which knows that Suncoast and Class members, as payment card issuers, lenders, and deposit account holders, bear the ultimate responsibility for identity theft and fraudulent lending and other consumer transactions.

22. Generally, financial institutions like Suncoast and Class members report to the credit reporting bureaus, including Equifax, on a monthly basis. Suncoast provides its customers' confidential information to Equifax so that Equifax may use its expertise to aggregate, process, and analyze the information, and market the information to the financial services industry and consumers directly. For example, financial institutions, like Suncoast, purchase the aggregated information from Equifax for purposes of analyzing the creditworthiness and financial condition of consumers. Equifax had a duty to properly secure its IT systems and website from hackers, use available technology to encrypt and otherwise secure consumers' PII and Payment Card Data using industry standard methods, and act reasonably to prevent the foreseeable harm to Suncoast and the Class, which it reasonably should have known would result from a data breach.

23. 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, which typically rely on the files at credit-reporting agencies, such as Equifax, to determine whether applications for consumer credit or loans are creditworthy. Not only has that process now been thrown into jeopardy for Suncoast and the Class, but such financial institutions also are now without a reliable, vital source of verifying consumers' identities due to the extent of the personal and financial information compromised by the Equifax Data Breach.

See Telis Demos, *Equifax Hack Could Slow Down Fast Loans*, WALL ST. J., Sept. 11, 2017, https://www.wsj.com/articles/equifax-hack-could-slow- down-fast-loans-1505147969.

24. The dire consequences of the increased risk of identity theft caused by Equifax's failures cannot be overemphasized. With the information used to establish a legal identity now available to identity thieves for over 145 million consumers, financial institutions are at a greatly increased risk of loan and deposit account fraud and payment card transaction fraud, and are left to devise, implement, and pay for their own prophylactic measures to reduce such risk.

25. For all of these reasons, the Equifax Data Breach has sent shockwaves throughout the entire financial services industry. Its reverberations will be felt for years to come as injury and damages are inflicted on financial institutions, such as Suncoast and the Class.

III. The Equifax Data Breach.

26. On September 7, 2017, Equifax announced a data breach event estimated to affect approximately 143 million U.S. consumers.

27. From at least May 13, 2017 to July 30, 2017, hackers exploited a vulnerability in Equifax's U.S. web server software to illegally gain access to certain consumer files. The attack vector used in the incident occurred through a vulnerability in Apache Struts (CVE-2017-5638), an open-source application

framework supporting the Equifax online dispute portal web application. Equifax, *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes* (Sept. 15, 2017), https:// www.equifaxsecurity2017.com/ 2017/09/15/ equifax-releases-details-cybersecurity-incident-announces-personnel-changes/.

28. The alleged May 13, 2017 start date is based on Equifax's public statements of the results of its own investigation. Other sources, including Visa and MasterCard, have suggested that the Breach may have started much earlier, as far back as November 2016.

29. The potential vulnerability of the Apache Strut software was no secret. Numerous entities identified and issued public warnings in March 2017 regarding its vulnerability, including The Apache Foundation, the U.S. Department of Commerce's National Institute of Standards and Technology ("NIST"), and the U.S. Department of Homeland Security's Computer Emergency Readiness Team ("U.S. CERT"). Apache and NIST described the flaw as "critical," which is the highest rating used to indicate the danger of such a vulnerability.

30. In the days that followed, media reports noted that hackers were already exploiting the vulnerability against various companies and government agencies. Dan Goodin, *Critical vulnerability under "massive" attack imperils high- impactsites*, ARSTECHNICA (March 9, 2017), https:// arstechnica.com/

information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/. Equifax has publicly stated that its security team "was aware of this vulnerability at that time [in March 2017]." *See Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra*.

31. On March 7, 2017, the same day the vulnerability was publicly announced, The Apache Foundation made various patches and workarounds available to protect against the vulnerability. *See* Elizabeth Weise and Nathan Borney, *Equifax Had Patch 2 Months Before Hack and Didn't Install It, Security Group Says*, USA TODAY (Sept. 14, 2017), https://www.usatoday.com/story/money/2017/09/14/equifax-identity-theft-hackers- apache-struts/665100001/. Despite the available patches and workarounds, Equifax affirmatively and actively continued to use the outdated version of the software for two and a half months without properly applying them or taking other measures to protect against the flaw. *Id*. Equifax's conduct in this regard constitutes active misfeasance.

32. On March 8, 2017, U.S. CERT sent Equifax a notice of the need to patch a particular vulnerability in the "Apache Struts" software used for its online disputes portal, where consumers can dispute items on their credit report. Smith Testimony at 2-3, *supra*.

33. Equifax admitted that although it disseminated the U.S. CERT notification on March 9, 2017, and requested that the Apache Struts software be

patched, the Equifax security department did not patch the software in response to the notification. *Id.* Equifax further admits that it was the unpatched vulnerability in the Apache Struts software that allowed hackers to access the purloined PII and Payment Card Data.

34. Over the multi-month period of the Equifax Data Breach, hackers accessed sensitive consumer information, including names, social security numbers, birth dates, addresses, and driver's license numbers (*i.e.*, PII). The compromised data contains complete profiles of consumers whose personal information was collected and maintained by Equifax.

35. In addition to accessing sensitive PII, the hackers also accessed what Equifax purports to be 209,000 consumer credit card numbers, and an estimated 182,000 dispute records containing additional PII. *See* AnnaMaria Andriotis, *et al., Equifax Hack Leaves Consumers, Financial Firms Scrambling*, FOXBUSINESS.COM (Sept. 8, 2017), http://www.foxbusiness.com/ features/ 2017/09/08/equifax-hack-leaves-consumers-financial-firms-scrambling.html. Equifax stated that it believes all consumer credit card numbers were accessed in one fell swoop in mid-May 2017.

36. The hackers were also able to access Equifax's back-end servers, which are connected to financial institutions and enable the parties to share information digitally. Michael Riley, *et al., Equifax Suffered a Hack Almost Five Months*

Earlier Than the Date It Disclosed, BLOOMBERG.COM (Sept. 18, 2017), https://www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed?cmpid=socialflow-twitter-business&utm_content=business&utm_campaign=socialflow-organic&utm_source=twitter&utm_medium=social. Such an intrusion has left credit issuers, including Suncoast, woefully exposed to the threat of hackers piggybacking off of Equifax's lax security and entering its partners' systems.

37. Equifax estimates that 145.5 million Americans were impacted by this Breach. *See* Hamza Shaban, *Equifax says 2.5 million more may have been swept up in massive data breach*, WASHINGTON POST (Oct. 2, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/10/02/equifax-says-2- 5-million-more-may-have-been-swept-up-in-massive-data- breach/?utm_term= .f1f77ea141dd. It has not speculated on the number of financial institutions put at risk by this Breach, and has only admitted to losing Payment Card Data for roughly 200,000 payment cards. However, card brand alerts that inform card issuers, such as Suncoast, have started rolling in. These alerts already have revised the supposed beginning date of the Breach from July 2017 all the way back to November 2016.

38. Equifax reportedly discovered the Data Breach on July 29, 2017. *See Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra*.

39. After Equifax discovered the Breach, but before Equifax disclosed it to the public, three high-level executives sold shares in the company worth nearly $1.8 million. Anders Melin, *Three Equifax Managers Sold Stock Before Cyber Hack Revealed,* BLOOMBERG.COM (Sept. 7, 2017), https://www.bloomberg.com/news/articles/2017-09-07/three-equifaxexecutives-sold-stock-before-revealing-cyber-hack. On August 1, 2017 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.

40. On August 2, 2017, Equifax revealed that it had hired the services of Mandiant, a cybersecurity firm, to internally investigate the Breach. *See Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra.* Equifax did not report the Breach to the public until September 7, 2017. To date, Equifax has not explained its delay in reporting the Breach to the public.

41. After Equifax revealed the Data Breach, it created a website, www.equifaxsecurity2017.com, to enable consumers to check whether they were potentially impacted by the Breach. Once a consumer disclosed additional highly sensitive information to Equifax, namely their last name and last six digits of their Social Security number, Equifax would inform the consumer whether he or she had

been impacted by the Breach.

42. On the same page that informed consumers whether they had been impacted, Equifax also directed them to a free identity theft protection and credit monitoring program provided by TrustedID, a wholly owned subsidiary of Equifax. By signing up for TrustedID, consumers were required to consent to settle any claims arising out of the use of TrustedID in arbitration, but retained their right to the trial of claims arising out of the Data Breach.

43. Commencing on September 9, 2017, and commensurate with its ineptitude regarding data security, Equifax erroneously directed consumers to a spoof website at least four times via Twitter. Janet Burns, *Equifax Was Linking Potential Breach Victims On Twitter to a Scam Site*, FORBES.COM (Sept. 21, 2017), https://www.forbes.com/ sites/janetwburns/2017/09/21/ equifax-was -linking-potential-breach-victims-on- twitter-to-a-scam-site/#bb68b87288f2. Rather than directing consumers to www.equifaxsecurity2017.com to determine whether consumer sensitive information was potentially compromised, Equifax mistakenly directed its Twitter followers to www.securityequifax2017.com, a website that was created by swapping the two words around and whose sole purpose was to highlight the vulnerabilities of the website Equifax created to assist potential victims.

44. Federal regulators announced they were investigating Equifax's delayed notification about the Breach. The FBI is also investigating the Breach,

and two congressional committees announced that they would hold hearings. *See* Andriotis, *supra*.

45. On September 13, 2017, Visa issued a CAMS alert stating that it had been notified by an acquirer of a potential network intrusion at Equifax that put Visa accounts at risk. The Visa CAMS alert indicated that the exposure window was approximately May 11, 2017 through July 26, 2017, and the payment card data that had been compromised included PAN, CVV2, expiration dates, and cardholder names. Visa further stated that financial institutions that received this CAMS alert should take necessary steps to prevent fraud and safeguard cardholders.

46. On September 15, 2017, Equifax announced the retirements of its Chief Information Officer and Chief Security Officer in connection with the Data Breach and its aftermath. *See Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra*.

47. Numerous states and state attorneys general have rebuked Equifax in the wake of the Breach. On September 18, 2017, New York Governor Andrew Cuomo directed the state's Department of Financial Services to develop a rule forcing credit reporting agencies to register with the state and comply with its cybersecurity requirements. *See* Ashley Southall, *Cuomo Proposes Stricter Regulations for Credit Reporting Agencies*, N.Y. TIMES (Sept. 18, 2017), https://www.nytimes.com /2017/09/18/nyregion/equifax-hack-credit-reporting-

agencies-regulations.html.

48. On September 19, 2017 attorneys general from 43 states and the District of Columbia sent a letter to Equifax, criticizing it for the Data Breach and its response. *See* Jack Suntrup, *Hawley, Madigan criticize Equifax in letter signed by other state attorneys general*, ST. LOUIS POST-DISPATCH (Sept. 19, 2017), http://www.stltoday.com/business/national-and-international/hawley-madigan- criticize-equifax-in-letter-signed-by-other-state/article_868a0dbf-1ec6-57e0-87a7- 6d008005f8f0.html.

49. The same day, Massachusetts Attorney General Maura Healey filed a suit against Equifax, seeking financial penalties and disgorgement of profits, alleging that Equifax failed to promptly notify the public of the Breach, failed to protect the personal data in its possession, and engaged in unfair and deceptive trade practices. *See* David Lynch, *Equifax faces legal onslaught from US states*, FINANCIAL TIMES (Sept. 21, 2017), https://www.ft.com/content/bf04768c-9e1b-11e7-8cd4- 932067fbf946.

50. On September 26, 2017, Equifax, amid intense criticism, announced the abrupt retirement of CEO Richard Smith less than three weeks after it disclosed the Data Breach to the public. *See* Hamza Shaban, *Equifax CEO Richard Smith steps down amid hacking scandal*, WASHINGTON POST (Sept. 26, 2017), https://www.washingtonpost.com/ news/the-switch/wp/ 2017/ 09/26/equifax-ceo-

retires-following-massive-data-breach/?utm_term=.995964f8571c.

51. On October 2, 2017, Equifax announced that Mandiant had completed its internal forensic analysis of the Data Breach. Mandiant determined that an additional 2.5 million consumer records may have been compromised, bringing the total number of potentially compromised accounts to 145.5 million. *See* Hamza Shaban, *supra.*

52. Upon information and belief, although several months have passed since Equifax discovered the Data Breach, the investigation is still ongoing and the identity of the hackers is still unknown.

53. The Equifax Data Breach is one of the largest data breaches in history, in terms of the number of people exposed and the sensitivity of the information compromised: "[t]he Equifax hack is potentially the most dangerous of all, though, because the attackers were able to gain vast quantities of PII— names, addresses, Social Security numbers and dates of birth—at one time." Andriotis, *supra.*

IV. The Equifax Data Breach resulted from its active mishandling of PII and Payment Card Data, and failure to properly and adequately secure its systems.

54. The Equifax Data Breach was the direct result of Equifax's active mishandling of its IT systems, and failure to properly and adequately secure its systems, which contained PII and Payment Card Data.

55. Equifax, in making affirmative decisions regarding its active

management of its IT systems, ignored warnings from security experts about the vulnerabilities in the Apache Strut software. Equifax also failed to update the software to its latest version. In a statement posted September 14, 2017, The Apache Software Foundation attributed the Equifax Data Breach to Equifax's "failure to install the security updates provided in a timely manner." *Id.*; The Apache Software Foundation, *MEDIA ALERT: The Apache Software Foundation Confirms Equifax Data Breach Due to Failure to Install Patches Provided for Apache Struts Exploit* (Sept. 14, 2017), https://blogs.apache.org/foundation/entry/media-alert-the-apache-software.

56. Equifax also admitted in public statements that hackers were able to access this data by exploiting a vulnerability in Equifax's U.S. website application.

57. Equifax should have recognized and identified the flaws in its data security and taken measures to fix these vulnerabilities. Given the fact that the only product Equifax sells is highly sought-after data of the highest sensitivity, Equifax had a duty to employ up-to-the-minute data security and use industry best practices to prevent a security breach.

58. Even before this incident, Equifax was on notice of potential problems with its web security. For example, a security researcher reported that hackers claimed to have illegally obtained credit card information from Equifax, which they were attempting to sell in an online database. *See* Andriotis, *supra*; *see also*

Thomas Fox-Brewster, *A Brief History of Equifax Security Fails*, FORBES.COM (Sept. 8, 2017), https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/ #6b43b0ea677c. Equifax had a duty to respond to such a report of a significant software security flaw—but didn't.

59. Despite Equifax's knowledge of these potential security threats, Equifax willfully (or at least negligently) chose not to enact appropriate measures to ensure the security of its consumer files, including the encryption of sensitive PII and Payment Card Data.

60. As Equifax's CEO admitted, Equifax did not reduce the scope of sensitive data retained in backend databases and did not maintain adequate vulnerability scanning and patch management processes and procedures, such as restrictions and controls for accessing critical databases; network segmentation between internet facing systems and backend databases and data stores; firewalls; file integrity monitoring; network, application, database, and system-level logging to monitor the network for unusual activity; and endpoint detection software to prevent exfiltration of data. Smith Testimony, *supra.*

61. The injury and harm inflicted on Suncoast resulting from Equifax's failure to adequately secure its computer systems and websites was at all times entirely foreseeable to Equifax.

62. Equifax is well aware of the costs and risks associated with payment

card fraud and identity theft, and is particularly aware that Suncoast and the Class members bear the ultimate responsibility for payment card fraud and identity theft, as well as the obligation to protect against it. In fact, on its website, Equifax lists "some of the ways identity theft might happen," including when identity thieves "steal electronic records through a data breach." *Id*., *How Does Identity Theft Happen?* https://www.equifax.com/ personal/education/identity-theft/how-doesidentity-theft-happen (last accessed Oct. 3, 2017).

63. Because Equifax is aware of the harm caused by payment card fraud and identity theft, it offers products aimed at protecting consumers from such illegal activity. For example, on its website, Equifax advertises its "Equifax Complete™ Premier Plan" as "Our Most Comprehensive Credit Monitoring and Identity Protection Product." *Id*., *How Does Identity Theft Happen?* https://www.equifax.com/personal/education/identity-theft/how-doesidentity-theft-happen (last accessed Oct. 3, 2017). The product promises to monitor consumers' credit scores, provide text message alerts when suspicious activity on consumer banking or credit card accounts occur, lock the consumer's credit file for unapproved third parties, and automatically scan suspicious websites for consumers' personal information.

64. Equifax was aware of the risk posed by its insecure and vulnerable website. It also was aware of the extraordinarily sensitive nature of the personal information it maintains and the impact a data breach would have on consumers and financial institutions – including Suncoast and the Class members.

V. Equifax violated federal data security and other industry standards.

65. The Equifax Data Breach is unique because safeguarding Suncoast's and consumers' highly sensitive PII and Payment Card Data is one of the few responsibilities Equifax has—especially since sensitive data is the only product in which the company trades. As a company that deals exclusively in sensitive data, Equifax had the clear legal duty to maintain the confidentiality of Suncoast's and consumers' sensitive PII and Payment Card Data, and prevent any third-party misuse or access to such information. Equifax's utter failure to safeguard and protect such information violated federal data security and other industry standards, as well as violating a clearly established legal duty not to act negligently when handling and storing PII and Payment Card Data.

VI. Equifax failed to Comply with Federal Trade Commission Requirements.

66. According to the FTC, the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act of 1914 ("FTC Act"), 15 U.S.C. §45.

67. In 2007, the FTC published guidelines establishing reasonable data security practices for businesses. The guidelines suggest that businesses should protect the personal customer information they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vender-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating fraudsters may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

68. The FTC also has published a document entitled, "FTC Facts for Business," highlighting the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control risks.

69. The FTC also has issued orders against businesses that failed to employ reasonable measures to secure customer data, which provide further guidance to businesses regarding their data security obligations.

70. In the months and years leading up to the Data Breach and during the course of the Breach itself, Equifax did not follow the guidelines recommended by the FTC. Further, by actively mishandling the security of its IT systems and failing to have reasonable data security measures in place, Equifax engaged in an unfair act

or practice within the meaning of Section 5 of the FTC Act.

VII. Equifax failed to comply with industry standards for data security.

71. The Payment Card Industry Security Standards Council promulgates minimum standards that apply to all organizations storing, processing, or transmitting Payment Card Data. These standards, known as the Payment Card Industry Data Security Standard ("PCI DSS"), are the industry standards governing the security of Payment Card Data. They set the minimum level of what must be done, not the maximum.

72. PCI DSS 3.2, the version of the standards in effect beginning in April 2016, impose the following 12 "high-level" mandates:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

PCI DSS 3.2 also sets forth detailed and comprehensive requirements that must be followed to meet each of the 12 mandates.

73. Among other things, PCI DSS required Equifax to properly secure Payment Card Data; not store cardholder data beyond the time necessary to authorize

a transaction; implement proper network segmentation; encrypt Payment Card Information at the point-of-sale; restrict access to Payment Card Information to those with a need to know; and establish a process to identify and timely fix security vulnerabilities. As discussed herein, Equifax failed to comply with each of these requirements.

VIII. Suncoast has been, is currently being, and will be harmed by the Equifax Data Breach.

74. The Equifax Data Breach has inflicted immediate, hard costs on Suncoast and Class members similar to other data breaches in which PII and Payment Card Information is compromised and stolen. This includes costs for payment card cancellation and replacement, coverage of fraud charges on affected accounts, costs of notifying customers, opening and closing affected accounts, lost interchange fees, and other damages.

75. Unlike other data breaches, however, the Equifax Data Breach has caused severe, long term damages in myriad other ways. Because Equifax provides services that are so core to the business functioning of credit extenders and lenders such as Suncoast and Class members, the true extent of the damage may take years to fully materialize. Immediately, however, Suncoast and Class members are faced with the costs of dealing with customers who freeze their credit, making it impossible to determine their creditworthiness for current or potential credit or loans or to comply with regulatory requirements. Suncoast and Class members also

are faced with the requirement that in order to carry out their business functions, they must exchange the most sensitive customer information with Equifax, a company that has proven to have no ability to secure data.

76. Furthermore, and perhaps most significantly, Suncoast and Class members also face the obligation to pay for the costs of identity theft and fraudulent credit and other accounts for which the consumer victims are not responsible. The certain impending risk of identity theft and loan fraud as a direct result of the Equifax Data Breach, and the protections which must be now put in place to limit such risks, represents significant harm to Suncoast and Class members.

77. Equifax actively mishandled its data security and IT systems, failed to follow industry standards, and failed to effectively monitor its security systems to ensure the safety of customer information. Equifax's substandard data security protocols and failure to adequately monitor for unauthorized intrusion caused consumers' PII and Payment Card Data to be compromised for months without detection.

78. Furthermore, Suncoast's own data security is now at an increased and certain impending risk of being breached due to hackers accessing Equifax's back-end servers that are connected to Suncoast's servers. The Data Breach has left Suncoast exposed to the threat of hackers piggybacking off of Equifax's insufficient security to attack those who do business with Equifax.

79. Suncoast has incurred, and will continue to incur, substantial damages because of Equifax's failures to meet reasonable standards of data security. Suncoast has had to immediately react to mitigate the fraudulent transactions being made on payment cards it had issued while simultaneously taking steps to prevent future fraud, including identity theft that will lead to loan fraud. Suncoast is also in a heightened state of alert and incurring significant administrative costs regarding its own data security as a result of the hackers' potential access to their networks via the digital connection shared with Equifax.

80. As a result of the Equifax Data Breach, Suncoast and the Class are required to cancel and reissue payment cards, change or close accounts, notify customers that their cards were compromised, investigate claims of fraudulent activity, refund fraudulent charges, increase fraud monitoring on their own networks as well as on potentially impacted accounts, go to greater lengths to verify the identity of consumers seeking loans in light of impending credit freezes, and take other steps to protect themselves and their customers—all in an effort to reduce the risk of future, but certainly impending, identity theft, loan fraud, and other fraudulent consumer transactions.

81. Suncoast and the Class also lost interest revenue and transaction fees due to reduced payment card usage. Furthermore, debit and credit cards belonging to Suncoast and the Class, as well as the account numbers on the face of the cards,

were devalued. This devaluation of the payment cards and the data set forth on them represents real, quantifiable damage to the property of Suncoast and the Class.

82. Sensitive personal and financial information, like the information compromised in the Breach, is extremely valuable to thieves and hackers. These criminals have gained access to complete profiles of individuals' personal and financial information. They can now use this data 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. A report by the Department of Justice found that 86% of identity theft victims in 2014 experienced the fraudulent use of existing account information, including credit card and bank account information. *See* Erika Harrell, *Victims of Identity Theft, 2014*, U.S. Department of Justice, Bureau of Justice Statistics, NCJ 248991 (Sept. 2015) at 1, https://www.bjs.gov/content/pub/pdf/vit14.pdf.

83. While consumers are ultimately protected from most fraud loss arising from this incident, Suncoast and the Class are not—they bear the primary responsibility for reimbursing customers for fraudulent charges, fraudulently opened

accounts, and covering the costs of issuing new payment cards for customers to use and implementing new customer security and authentication procedures. Suncoast and the Class also will suffer financial losses whenever an identity is stolen and used to falsely establish credit, create a deposit account, or access an existing customer's account. This certainly impending risk will continue into the foreseeable future, and require Suncoast and the Class to incur significant costs and expenses in order to reduce and mitigate it.

84. Financial institutions are responsible for all charges to fraudulently opened accounts. When complete consumer profiles are compromised, financial institutions experience continuous losses as identity thieves move on from one consumer profile to the next. With a data breach of this magnitude, there is virtually no limit to the amount of fraudulent account openings Suncoast and the Class may face. These risks are very real in the wake of the Equifax Data Breach and certainly impending.

85. As a result of the Equifax Data Breach, 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, institute new customer security and authentication procedures, 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.

86. Consumers inevitably 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 Breach. *Id.* This stress also impacts financial institutions, which are forced to expend additional customer service resources helping their concerned 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, and other charges that they may have otherwise collected on these accounts.

87. In addition, financial institutions have and will continue to incur significant costs in implementing additional customer authentication methods, such as, for example, multi-factor customer authentication. These measures are necessary as a direct and mitigating response to the Equifax Data Breach.

88. Financial institutions will also face increased regulatory compliance costs going forward as a result of the Breach. 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 administrative costs of these additional measures.

89. Financial institutions also will be harmed by the chilling effect the Breach will have on future lending as consumers deal with its impact on their finances and credit. Customers or members are often without access to their accounts for several days at a time while payment cards are replaced or accounts are changed. Some customers also are hesitant to use payment card transactions altogether in the wake of a major breach. This results in lost fees and interest to the financial institutions issuing these cards—including Suncoast and the Class.

90. Financial institutions are also harmed by the chilling effect the Breach will have on consumers' willingness to seek extensions of credit through instruments, such as home mortgages and credit cards. Customers who do not react to the Breach by placing a freeze on their credit may nevertheless refrain from obtaining credit in its wake, which will result in lost fees and interest to financial institutions—including Suncoast and the Class.

91. The massive and destabilizing Data Breach also threatens to severely disrupt the usual business operations of nearly every financial institution in the nation because they rely on Equifax to provide services that are core to the

institutions' credit extension, lending, and other functions. The inability to reliably exchange the information underlying these functions inflicts great, and real, risk and uncertainty to financial institutions' business models.

92. As a result of the Breach, financial institutions—including Suncoast and the Class—also have incurred significant costs in notifying their customers and responding to Breach-related inquiries.

93. Even more worrisome, financial institutions are often required to demonstrate the health of their credit and loan portfolios to regulators who require credit reports be pulled to analyze the strength of the portfolio. Such regulatory requirements cannot be met where multitudes of consumers have implemented credit freezes, which are cumbersome and costly to switch on and off.

94. Ultimately, Suncoast and the Class are faced with considerable present injury, and an immediate future of continually unfolding new and continued injuries as a result of the Data Breach that was easily avoidable.

IX. Equifax had a clear legal duty to prevent and timely report the Breach.

95. Equifax had a legal duty – owed to Suncoast and other financial institutions that bear the readily foreseeable risk of injury – to prevent a breach of consumers' sensitive PII and Payment Card Data.

96. Following several high-profile data breaches in recent years, including Target, Experian, Yahoo, Home Depot, and Sony, Equifax was on notice of the very

real risk that hackers could exploit vulnerabilities in its data security—even though Equifax has considerable resources to devote to ensuring adequate data security.

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

98. Suncoast and other financial institutions were harmed not only by the Breach, but also by Equifax's failure to timely report the Breach to the public.

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

100. An anonymous source familiar with the investigation stated:

> 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.

Id. But Equifax has not yet given an official explanation for its delay in reporting the Breach to the public. In the time between when Equifax discovered the Breach and when it reported the Breach to the public, however, three of its top executives sold substantial amount of Equifax stock, presumably avoiding the financial losses associated with the negative press Equifax has received since the Breach. In fact, the Equifax stock price 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 ST. J. (Sept. 8, 2017), https:// blogs.wsj. com/moneybeat/2017/09/08/equifaxshares-on-pace-for-worst-day-in-18-years/.

101. Because of this delay, consumers with compromised PII and Payment Card Data were unable to adequately protect themselves from potential identity theft for several weeks. The consequences to financial institutions from this delay are very real given that they ultimately bear financial responsibility for the fraud inflicted upon consumers.

102. Financial institutions have been unable to alert their members or customers of the risk in a timely manner, or implement measures to detect and prevent potential fraud in the time before the Breach was disclosed. Equifax's failure to report the Breach in a timely manner has resulted in additional harm to Suncoast and the Class.

X. Equifax has a history of poor data security.

103. Even before the Data Breach, Equifax was on notice of potential problems with its web security because of multiple security breaches Equifax has suffered in the past.

104. In April 2016, for example, hackers exploited Equifax's W-2 Express website, an Equifax service for companies to make electronic W-2 forms accessible to employees, and accessed sensitive tax data. Through an online portal, the hackers only had to enter an employee's default PIN code, which was simply the last four digits of the employee's Social Security number, and the employee's four-digit birth year. More than 400,000 employees' W-2 tax information was left open

to theft. *See* Brian Krebs, *Crooks Grab W-2s from Credit Bureau Equifax*, KREBS ON SECURITY (May 16, 2016), https://krebsonsecurity.com/2016/05/crooks-grab-w-2s- from-credit-bureau-equifax/.

105. The use of simple and easily identifiable information for a default login and password to access sensitive personal and financial data is a substandard security practice. Indeed, shortly after Equifax publicly announced the Breach, security researchers discovered that one of Equifax's online employee portals could be accessed by using the word "admin" for both the login and password. Once logged in through the portal, a user could easily access sensitive employee and consumer data. *See* Brian Krebs, *Auyda Help Equifax Has My Data*, KREBS ON SECURITY (Sept. 17, 2017), https://krebsonsecurity.com/ 2017/09/ayuda-help-equifax-has-my-data/.

106. For years, security researchers also have questioned Equifax's use of an easily identifiable security PIN issued to consumers who have locked their credit report. When a consumer requests a credit lock, Equifax provides a security PIN the consumer can then later use to unlock his or her credit. Instead of providing a secure, randomized PIN, Equifax only issues a date-time stamp of when the consumer requested the lock. Such an easily discernible PIN vastly increases the odds of someone attempting to unlock a credit report for the purposes of identity theft. Equifax has recently stated it is taking steps to provide randomly generated

PINs. *See* Sean Gallagher, *Equifax Moves To Fix Weak PINs For 'Security Freez' On Consumer Credit Reports*, ARSTECHNICA (Sept. 11, 2017), https://arstechnica.com/information-technology/2017/09/equifax-moves-to-fix-weak-pins-for-security-freeze-on-consumer-credit-reports/.

107. The impact of such weak security practices often results in the exploitation of consumer information in the black market. As one security researcher reported, hackers claimed to have illegally obtained credit card information from Equifax, which they were attempting to sell in an online database. *See* Andriotis, *supra*; *see also* Thomas Fox-Brewster, *A Brief History of Equifax Security Fails*, FORBES (Sept. 8, 2017), https://www.forbes.com/ sites/thomasbrewster/ 2017/09/08/equifax-databreach-history/#63dc4270677c.

CLASS ACTION ALLEGATIONS

108. Suncoast brings this action on behalf of itself and the following Nationwide Class under FED. R. CIV. P. 23(a); (b)(2); and (b)(3):

> All credit unions, banks financial institutions, and other entities in the United States (including its Territories and the District of Columbia) that issue payment cards and/or otherwise extend credit to consumers whose data was exposed, between May 2017 and July 2017, as a result of the Equifax Data Breach.

109. Should the Nationwide Class not be certified, Suncoast brings this action on behalf of itself and the following Florida Class under FED. R. CIV. P. 23(a); (b)(2); and (b)(3):

> All credit unions, banks financial institutions, and other entities in the State of Florida that issue payment cards and/or otherwise extend credit to consumers whose data was exposed, between May 2017 and July 2017, as a result of the Equifax Data Breach.

Should this action proceed as a certified Florida Class, Suncoast intends to assert all of its available claims and causes of action under Florida statutory and common law and in equity.

110. This action may properly be maintained as a class action because it satisfies the requirements of FED. R. CIV. P. 23(a): numerosity, commonality, typicality, and adequacy.

111. Numerosity. The Class members are so numerous that joinder would be impracticable. Suncoast believes there are over 10,000 Nationwide Class members, and over 400 Florida Class members.

112. Commonality. There are common questions of law and fact predominating over questions affecting only individual Class members, including, without limitation:

a. whether Equifax owed a duty to Suncoast and the Class members to protect PII and Payment Card Data;

b. whether Equifax failed to provide reasonable security to protect PII and Payment Card Data;

c. whether Equifax negligently or otherwise improperly allowed PII and Payment Card Data to be accessed by third parties;

d. whether Equifax failed to adequately notify Suncoast and the Class

members that its data systems were breached;

e. whether Suncoast and the Class members were injured and suffered damages and ascertainable losses;

f. whether Equifax's failure to provide reasonable security proximately caused the injuries suffered by Suncoast and the Class members;

g. whether Suncoast and the Class members are entitled to damages and, if so, the measure of such damages; and

h. whether Suncoast and the Class members are entitled to declaratory and injunctive relief.

113. Typicality. Suncoast's claims are typical of the claims of the absent Class members and have a common origin and basis. Like Suncoast, absent Class members are financial institutions injured by the Equifax Data Breach. Suncoast's claims arise from the same practices and course of conduct giving rise to the claims of the absent Class members and are based on the same legal theories—namely, the Equifax Data Breach. If prosecuted individually, each Class member's claims would necessarily rely upon the same material facts and legal theories, and seek the same relief. Suncoast's claims arise from Equifax's same wrongful practices and course of conduct giving rise to the other Class members' claims, and are based on the same legal theories.

114. Adequacy. Suncoast will fully and adequately assert and protect the interests of the absent Class members and has retained counsel experienced in data breach litigation and qualified to prosecute class action cases similar to this one.

Neither Suncoast, nor their attorneys, have any interests contrary to, or conflicting with, the interests of absent Class members.

115. The questions of law and fact common to all Class members predominate over any questions affecting only individual class members.

116. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the absent Class members' claims is economically infeasible and procedurally impracticable. Class members share the same factual and legal issues, and litigating the claims together will prevent varying, inconsistent, or contradictory judgments, and prevent the delay and expense to the parties and the court system associated with litigating multiple trials on the same legal and factual issues. Class treatment also will permit Class members to litigate their claims that otherwise might be too expensive or inefficient to do so. Suncoast knows of no difficulties in managing this action that would preclude it from being litigated as a class action. This action, therefore, satisfies all of the requirements of FED. R. CIV. P. 23(b)(3).

117. This action also satisfies all of the requirements of FED. R. CIV. P. 23(b)(2). Equifax, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, thereby making injunctive and declaratory relief appropriate to the Class as a whole.

CLAIMS AND CAUSES OF ACTION

COUNT I
Negligence
(On behalf of Suncoast and the Nationwide Class, or, in the alternative, on behalf of Suncoast and the Florida Class)

118. The preceding allegations are incorporated herein by reference.

119. Equifax owed – and continues to owe – a duty to Suncoast and Class members to use reasonable care in safeguarding PII and Payment Card Data and notify them of any data breach in a timely manner so that appropriate action could be taken to minimize or avoid losses. This duty arises from several sources, including, without limitation, the sources described below, and is independent of any duty Equifax owed as a result of any contractual obligations.

120. Equifax has a common law duty to prevent the foreseeable risk of harm to others, including Suncoast and Class members. The duty to protect others against the risk of foreseeable criminal conduct has been recognized in situations in which parties are in a special relationship, or where an actor's conduct or misconduct exposes another to a risk, or defeats protections put in place to guard against a risk. *See* RESTATEMENT (SECOND) OF TORTS §302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard PII, Payment Card Data, and other sensitive information.

121. It was foreseeable that injury would result—and, in fact, resulted—from Equifax's failure to use reasonable measures to protect PII and Payment Card

Data and provide timely notice of the Breach. It also was foreseeable that if reasonable data security measures were not taken, hackers would steal PII and Payment Card Data belonging to millions of consumers, and use the PII and Payment Card Data to inflict the injury and damages described herein.

122. There is no question that the prevalence of data breaches and identity theft has increased dramatically in recent years in the U.S., accompanied by a parallel and growing economic drain on the victimized individuals, businesses, and government entities. According to the Identity Theft Resource Center, in 2016, there was a total of 1,093 reported data breaches in the United States, an all-time high. Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), http://www.idtheftcenter.org/2016databreaches.html. More than 36 million records were reportedly exposed in those breaches. Identity Theft Resource Center, *Data Breach Reports: 2016 End of Year Report (*Jan. 18, 2017) at 226, http://www. idtheftcenter.org/images/breach /2016/DataBreachReport_ 2016.pdf.

123. It is well known that a common motivation of data breach perpetrators is the hackers' intentions to sell PII and/or Payment Card Data on underground black markets, and news outlets reported that this, in fact, occurred after the Home Depot and Target data breaches, among others. Malicious or criminal attacks were the cause of 50% of the breaches covered by the IBM study, and were

also the most costly. *Id*. at 8.

124. In tandem with the increase in data breaches, the rate of identity theft also reached record levels in 2016, affecting approximately 15.4 million victims in the United States and causing approximately $16 billion of fraud losses. Javelin Strategy & Research, *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study* (Feb. 1, 2017), https://www. javelinstrategy.com/ press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent- according-new. In this environment, every reasonable person and company in the United States is aware of the significant risk of criminal attacks against computer systems that store PII, Payment Card Data, and other sensitive and confidential information.

125. Equifax assumed the duty to use reasonable security measures consistent with its conduct, internal policies and procedures, and Privacy Policy in which the company stated it used "industry standard means" of protecting PII and Payment Card Data, and its security measures were "appropriate for the type of information we collect." By means of these statements, Equifax specifically assumed the duty to comply with industry standards, including PCI DSS and every other conceivable standard applicable to a company whose sole business is transacting in the most sensitive consumer information in existence.

126. Equifax's duty to use reasonable security measures also arose from

the special relationship that existed between Equifax, Suncoast, and the Class. The special relationship exists because financial institutions entrusted Equifax with customer PII and Payment Card Data. Only Equifax was in a position to ensure that its systems were sufficient to protect financial institutions—such as Suncoast—from the injury and harm inflicted by a data breach.

127. Equifax's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by retailers, such as Equifax. FTC publications and data security breach orders further form the basis of Equifax's duty. Individual states also have enacted statutes based upon the FTC Act creating such a duty.

128. Equifax's duty to use reasonable care in protecting PII and Payment Card Data arose not only as a result of the common law and the statutes described above, but also because it was bound by, and had committed to comply with, industry standards, specifically including PCI DSS.

129. Equifax breached its common law, statutory, and other duties – and was negligent – by failing to use reasonable measures to protect consumers' PII and Payment Card Data from the hackers who perpetrated the Data Breach and by failing to provide timely notice of the Breach. The specific negligent acts and

omissions committed by Equifax include, without limitation:

a. failing to employ reasonable systems to protect against malware;

b. failing to regularly and reasonably update its antivirus software;

c. failing to maintain an adequate firewall;

d. failing to reasonably track and monitor access to its network and consumer data;

e. failing to reasonably limit access to those with a valid purpose;

f. failing to heed warnings about specific vulnerabilities in its systems identified by Equifax's own employees, consultants, and software vendors;

g. failing to recognize red flags signaling that Equifax's systems were inadequate and, as a result, the potential for a massive data breach akin to the one involving Target and Home Depot was increasingly likely;

h. failing to recognize that hackers were stealing PII and Payment Card Data from its systems while the Breach was taking place; and

i. failing to disclose the Data Breach in a timely manner.

130. As a direct and proximate result of Equifax's negligence, Suncoast and the Class members have suffered, and will continue to suffer, the injury, harm, and damages described herein.

131. As a direct and proximate result of Equifax's negligence, Suncoast and the Class have suffered, and will continue to suffer, injury as described herein.

132. Because no statutes of other states are implicated, Georgia common law applies to the negligence claims of Suncoast and Class members.

COUNT II
Negligence *Per Se*
(On behalf of Suncoast and the Nationwide Class,
or, in the alternative, on behalf of Suncoast and the Florida Class)

133. The preceding allegations are incorporated herein by reference.

134. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by consumer-serving organizations, such as Equifax, of failing to use reasonable measures to protect PII and Payment Card Data. The FTC publications and orders described above also form the basis of Equifax's duty.

135. Equifax violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and Payment Card Data and not complying with applicable industry standards, including PCI DSS. Equifax's conduct was particularly unreasonable given the nature and amount of PII and Payment Card Data it obtained and stored, and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result (and have resulted) to consumers and financial institutions (such as Suncoast).

136. Equifax's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

137. Suncoast and the Class members are within the scope of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect as they

are engaged in trade and commerce and bear primary responsibility for paying, and reimbursing consumers, for fraud losses. Moreover, many Class members are credit unions organized as cooperatives whose members are consumers—such as Suncoast.

138. The injury and harm inflicted on financial institutions by the Data Breach is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and abstain from unfair and deceptive practices, inflicted the same injury and harm inflicted by Equifax on Suncoast and the Class members.

139. As a direct and proximate result of Equifax's negligence *per se*, Suncoast and the Class members have suffered, and will continue to suffer, the injury, harm, and damages described herein.

140. Because no statutes of other states are implicated, Georgia common law applies to the negligence *per se* claim of Suncoast and the Class members.

COUNT III
Declaratory and Equitable Relief
(On Behalf of Suncoast and the Nationwide Class,
or, in the alternative, on behalf of Suncoast and the Florida Class)

141. The preceding allegations are incorporated herein by reference.

142. Under the Declaratory Judgment Act, 28 U.S.C. §2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the

parties, and grant further necessary relief. The Court also has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this complaint.

143. An actual controversy exists in the wake of the Equifax Data Breach regarding its common law and other duties to reasonably safeguard its customers' PII and Payment Card Data. Suncoast alleges that Equifax's data security measures were inadequate and remain inadequate. Suncoast also continues to suffer injury and damages as described herein.

144. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, that:

a. Equifax continues to owe a legal duty to secure PII and Payment Card Data under, *inter alia*, the common law and Section 5 of the FTC Act;

b. Equifax continues to breach its legal duty by failing to employ reasonable measures to secure PII and Payment Card Data; and

c. Equifax's ongoing breaches of its legal duty continue to inflicy injury and harm on Suncoast and Class members.

145. The Court should also issue the following corresponding injunctive relief requiring Equifax to employ adequate security protocols consistent with industry standards to protect PII and Payment Card Data Among other things, the Court should direct Equifax to:

a. implement encryption keys in accordance with industry standards;

b. consistent with industry standards, engage third party auditors to test its systems for weaknesses and upgrade any such weaknesses if found;

c. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

d. regularly test its systems for security vulnerabilities, consistent with industry standards; and

e. install all upgrades recommended by manufacturers of security software and firewalls used by Equifax.

146. If an injunction is not issued, Suncoast and Class members will suffer irreparable injury without an adequate legal remedy in the event of another data breach at Equifax, which is a real possibility given the continued missteps taken by Equifax described herein, including using its official corporate communications to send affected consumers to phishing sites. Indeed, Equifax was hit with a separate data breach in March 2017 that apparently did nothing to motivate the company to discover this Data Breach going on at the same time. *See* Mark Coppock, *Equifax Confirms It Suffered A Separate Data Breach In March*, DIGITAL TRENDS (Oct. 3, 2017), https://www.digitaltrends.com/computing/ equifax-data-breach-affects-143-million-americans/.

147. The risk of another Equifax data breach is real, immediate, and substantial. If another Equifax data breach should occurs, Suncoast and Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable and they will be forced to bring multiple

lawsuits to rectify Equifax's same egregious conduct.

148. If an injunction does not issue, the hardship to Suncoast and Class members would exceed the hardship to Equifax if an injunction is issued. Among other things, if another massive data breach occurs at Equifax, Suncoast and Class members will likely incur millions of dollars in damages. On the other hand, the cost to Equifax of complying with an injunction by employing reasonable data security measures that Equifax already has a legal obligation to employ is relatively minimal.

149. Issuance of the requested injunction will serve the public interest by preventing another Equifax data breach, thereby eliminating the injury, harm, and damages that would be inflicted on Suncoast, Class members, and the potentially millions of consumers whose PII and Payment Card Data would be compromised.

RELIEF REQUESTED

WHEREFORE, Suncoast, individually and on behalf of Class members, respectfully requests the Court to:

a. certify the Nationwide Class, or, in the alternative, certify the Florida Class, and appoint Suncoast and Suncoast's counsel to represent the Class;

b. enter a monetary judgment against Equifax in favor of Suncoast and the Class to compensate them for the injury, harm, and damages they have suffered, and will continue to suffer as a direct and/or proximate result of the

Equifax Data Breach;

c. award Suncoast and the Class punitive damages, treble damages, statutory damages, and penalties where appropriate;

d. award Suncoast and the Class pre-judgment and post-judgment interest at the highest legal rates;

e. enter a declaratory judgment as described herein and corresponding injunctive relief requiring Equifax to employ adequate security protocols consistent with industry standards to protect PII and Payment Card Data;

f. award Suncoast and the Class their attorneys' fees, litigation expenses, and costs of suit; and

g. award Suncoast and the Class such other and further relief that this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff Suncoast Credit Union respectfully demands a trial by jury on all claims so triable.

Date: January 30, 2018

Respectfully submitted,

By: /s/*Reginald L. Snyder*
Reginald L. Snyder
DYE SNYDER, LLP
260 Peachtree St. NW, Suite 502
Atlanta, GA 30303
Telephone: (678) 974-8360
Facsimile: (404) 393-3872
Email: rsnyder@dyesnyder.com

Richard L. Coffman
THE COFFMAN LAW FIRM
First City Building
505 Orleans St., Fifth Floor
Beaumont, TX 77701
Telephone: (409) 833-7700
Facsimile: (866) 835-8250
Email: rcoffman@coffmanlawfirm.com

COUNSEL FOR PLAINTIFF SUNCOAST CREDIT UNION

LOCAL RULE 7.1(D) CERTIFICATION

Pursuant to Local Rule 7.1(D), I hereby certify that this Complaint was prepared with the font and point selections (Times New Roman, 14 point) approved by the Court in Local Rule 5.1(C).

/s/*Reginald L. Snyder*
Reginald L. Snyder
DYE SNYDER, LLP
260 Peachtree St. NW, Suite 502
Atlanta, GA 30303
Telephone: (678) 974-8360
Facsimile: (404) 393-3872
Email: rsnyder@dyesnyder.com

COUNSEL FOR PLAINTIFF SUNCOAST CREDIT UNION

JS 44 (Rev. 06/17)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

SUNCOAST CREDIT UNION, individually and on behalf of all other similarly situated financial institutions

(b) County of Residence of First Listed Plaintiff Hillsborough County, FL
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Reginald Snyder, Dye Snyder, LLP, 260 Peachtree St. NW, Ste 502, Atlanta, GA 30303, (404) 678-7032; Richard Coffman, The Coffman Law Firm, 505 Orleans St., 5th FL, Beaumont, TX 77701, (409) 833-7700

DEFENDANTS

EQUIFAX, INC.

County of Residence of First Listed Defendant Fulton County, GA
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☒ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☒ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
Fair Credit Reporting Act, 15 U.S.C. §1681

Brief description of cause:
Data breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
01/30/2018

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____