IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

CHRIS TOSCO, and MARK ASHLEY, Individually and on behalf of all others similarly situated, Plaintiffs, vs. EQUIFAX INC., a Georgia Corporation, Defendant.	Case No.:

CLASS ACTION COMPLAINT

I. INTRODUCTION

1. Equifax Inc. ("Equifax"), is a global corporation that organizes, assimilates, and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide. Founded in 1899 as a small-scale data collector, Equifax has since grown into a data aggregation behemoth and one of the "Big Three" credit reporting agencies, collecting billions of individual pieces of data on consumers annually – decades worth of addresses, driver's license numbers, social security numbers, utility accounts, telephone and cable subscriptions, criminal records, medical debt, and more.

2. As the collector and holder of the sensitive personal and financial information of hundreds of millions of individuals – usually without their knowledge or consent – Equifax had a duty to ensure that the sensitive information it possessed was protected from unauthorized persons seeking to use that data for illegitimate and harmful purposes. Indeed, it was a duty that Equifax recognized and used to its advantage, touting itself as a steward and industry leader in data security and earning billions of dollars in revenue generated from products and services sold to consumers and business alike, related to credit reports and monitoring, and identity-theft protection.

3. But what Equifax's customers and the tens of millions of Americans on whom Equifax had collected and stored information did not know, and could not know, was that the self-proclaimed leader in managing and protecting data did not have the most secure and up-to-date security protecting its own systems. Nor did they know that Equifax would fail to detect the vulnerability in its systems and fail to effectively and promptly patch critical software necessary to address the vulnerability, despite the patches being available and the vulnerability in the software used by Equifax widely reported. And when a data breach involving records of close to 146 million innocent consumers occurred, the 146 million Americans whose information was compromised could not know that Equifax would fail to immediately and accurately notify all those affected to prevent them from becoming victims of identity theft. Yet, that is precisely what Equifax did.

4. Equifax failed to ensure that thieves and hackers could never get access to the data the agency has collected. It failed to repair and patch critical software it used in its systems effectively and promptly, despite the multitude of media reports that the specific software used by Equifax was vulnerable to attack and a patch addressing the vulnerability was available. And when the data breach affecting 146 million Americans inevitably occurred, Equifax failed to immediately and accurately notify those Americans or take other measures designed to mitigate the damage that it was ultimately responsible for. Now, tens of millions of Americans' personal and financial data are compromised and will never again be secure. Accordingly, Plaintiffs Chris Tosco and Mark Ashley bring this class action lawsuit on behalf of themselves and all others similarly situated whose data was compromised and identities stolen due to Equifax's conduct.

II. PARTIES, JURISDICTION AND VENUE

5. Plaintiff Chris Tosco is a citizen and resident of Miami-Dade County, Florida, and was a citizen and resident of Florida between mid-May 2017 through July 2017, when, according to Equifax, the data breach occurred. Plaintiff Tosco was also a citizen and resident of Florida on or around July 29, 2017, when Equifax reported that it had learned of the data breach. Plaintiff Tosco accessed the Defendant's website to assess whether his personal information was compromised by the data breach. Upon using Equifax's "Am I Impacted?" tool at www.equifaxsecurity2017.com/am-i-impacted/, Plaintiff Tosco learned that his personal information may have been stolen in the data breach. Plaintiff Tosco then enrolled in the Equifax credit monitoring service. Additionally, Plaintiff Tosco intends to pay for credit freezes at all three credit bureaus.

6. Plaintiff Mark Ashley is a citizen and resident of Los Angeles, California, and was a citizen and resident of California between mid-May through July 2016, when, according to Equifax, the data breach occurred. Plaintiff Ashley was also a citizen and resident of California on or around July 29, 2017, when Equifax reported that it had learned of the data breach. Plaintiff Ashley accessed the Defendant's website to assess whether his personal information was compromised by the data breach. Upon using Equifax's "Am I impacted?" tool at www.equifaxsecurity2017.com/am-i-impacted/, Plaintiff Ashley learned that his personal information may have been stolen in the data breach. Plaintiff Ashley intends to enroll in the Equifax credit monitoring service and to pay for credit freezes at all three credit bureaus.

7. Defendant Equifax is a Georgia corporation with its principal place of business in Atlanta, Georgia. Equifax organizes, assimilates, and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide. Equifax provides credit and

demographic related data and services to business and sells credit monitoring and fraud-prevention services directly to consumers. In 2016, Equifax's revenues exceeded $3 billion.

8. The Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A), because this is an action for a sum exceeding $5,000,000, exclusive of interests and costs, and at least one class member is a citizen of a state different than that of the Defendant.

9. This Court has jurisdiction over Equifax because Equifax continuously and systematically operates, conducts, engages in or carries on a business or business venture in Florida. Moreover, Equifax engages in substantial and not isolated activity within this State and therefore is subject to the jurisdiction of the courts within this State. Accordingly, Equifax is subject to Florida's long arm jurisdiction under § 48.193, Fla. Stat. (2016).

10. Venus is proper in this district pursuant to 28 U.S.C. §1391(b) because Equifax regularly conducts business within this district and is subject to the personal jurisdiction of the courts within this district, Plaintiff Tosco resides in this district, and property that is the subject of Plaintiff Tosco's claims are in this district.

III. FACTUAL ALLEGATIONS

11. Equifax is one of the three major credit reporting agencies that collect, track and rate the financial history of individuals across the nation and worldwide. Equifax aggregates data about loans, loan payments, credit cards, child support payments, banking information, credit limits, missed payments, credit inquiries, employer histories, addresses, social security numbers, birthdays, and more. In short, Equifax collects and holds a massive amount of sensitive personal information about tens of millions of individuals, often without the individuals' knowledge or consent.

12. On September 7, 2017, Equifax disclosed to the general public that its computer systems had been hacked. Equifax stated that "[c]riminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017."[1]

13. The breach impacted "approximately 143 million U.S. consumers" – nearly half the country's population – and the information accessed "include[d] names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers.[2] In fact, the driver's license data belonging to approximately 10.9 million people was obtained by criminals during the breach.[3] In addition, "credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed."[4]

14. Equifax further admitted that it did not detect the breach until July 29, 2017, despite the breach occurring as early as mid-May. Thus, Equifax, a company whose business is the collection and storage of sensitive data and whom millions of consumers depend on to guard against identity theft, admitted that its systems were compromised for roughly two and a half months before it had any idea it had been hacked. Even worse, Equifax did not disclose to the public the breach it had finally discovered until September 7, 2016, almost six weeks later. It most

[1] *Equifax Announces Cybersecurity Incident*, EQUIFAX (Sept. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.
[2] *Id.*
[3] Harper Neidig, *Equifax Breach Exposed Driver's License Data*, THEHILL.COM (Oct. 11, 2017), http://thehill.com/policy/technology/354893-equifax-breach-exposed-driver-license-data-for-nearly-11m-americans-report.
[4] *Equifax Announces Cybersecurity Incident*, *supra* note 1.

recently announced that a forensic investigation revealed that an additional 2.5 million U.S. consumers had been impacted by the breach, bringing the total to 145.5 million.[5]

15. The worst part, however, is that the breach was fully preventable. Equifax had notice of the software vulnerability that allowed the theft of data belonging to approximately 146 million Americans for some two months before the breach occurred. Indeed, there were press reports of widespread attempts by hackers to exploit this vulnerability. Yet, Equifax failed to take the steps necessary to secure the trove of consumers' personal information it possessed or to seal off any outside access to it while Equifax worked on a fix, assuming Equifax ever made any effort to do so.

16. On September 15, 2017, Equifax announced that "the attack vector used in this incident occurred through a vulnerability in Apache Struts (CVE-2017-5638), an open-source application framework that supports the Equifax online dispute portal web application."[6]

17. That particular vulnerability, however, was addressed in early March 2017, with patches becoming available at that time to everyone who uses Struts.[7] Thus, Equifax had the means by which to fix the problem months before the breach occurred but neglected to do so.

18. As Ars Technica reported on September 13, 2017, "the flaw in the Apache Struts framework was fixed on March 6. Three days later, the bug was already under mass attack by hackers who were exploiting the flaw to install rogue applications on Web servers. Five days after

[5]*Equifax Announces Cybersecurity Firm has Concluded Investigation*, EQUIFAX (Oct. 2, 2017), https://investor.equifax.com/news-and-events/news/2017/10-02-2017-213238821.
[6]*Equifax Announces Personnel Changes* (Sept. 15, 2017), https://www.equifaxsecurity2017.com/2017/09/15/equifax-releases-details-cybersecurity-incident-announces-personnel-changes/.
[7]David Meyer, *Equifax's Mega-Breach Made Possible by Fixable Website Flaw*, FORTUNE MAG. (Sept. 14, 2017), http://fortune.com/2017/09/14/equifax-data-breach-security-apache-struts/.

that, the exploits showed few signs of letting up."[8] Equifax's belated disclosure of the massive breach and its cause "strongly suggests that Equifax failed to update its Web applications, despite demonstrable proof that the bug gave real-world attackers an easy way to take control of sensitive sites."[9]

19. "This vulnerability was disclosed back in March," said Bas van Schaik, a product manager and researcher at Semmle, an analytics security firm. "There were clear and simple instructions of how to remedy the situation. The responsibility is then on companies to have procedures in place to follow such advice promptly."[10] "The fact that Equifax was subsequently attacked in May means that Equifax did not follow that advice. Had they done so this breach would not have occurred."[11]

20. Thus, despite the issuance of a patch, publicity about the barrage of attacks attempting to exploit the reported vulnerability, and the extremely sensitive personal and financial information gathered and stored by Equifax, Equifax neglected to take the steps necessary to neutralize the possibility of its systems getting hacked. The result is the massive data breach that will likely have serious consequences – perhaps for decades – for 145.5 million Americans.

21. Then, instead of promptly notifying the nearly 146 million consumers whose complete identity information was stolen by "criminals," Equifax stayed silent, leaving the stolen data in the hands of those criminals, and the victims in the dark about their vulnerability, for at least three months between the time the breach began and the time Equifax finally disclosed it to

---

[8]Dan Goodin, *Failure to Patch Bug Led to Massive Equifax Breach*, ARS TECHNICA (Sept. 13, 2017), https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/.

[9]*Id.*

[10]Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED.COM (SEPT. 14, 2017), https://www.wired.com/story/equifax-breach-no-excuse/.

[11]*Id.*

the public. Equifax plainly did not take the necessary and reasonable steps to protect its data storage systems from a known and fixable vulnerability, which allowed the attack, and it failed to promptly notify affected consumers once it learned of it.

22. Of course, two days after Equifax detected the breach, company executives sold over $1.8 million of Equifax stock before any negative new could cause a stock collapse, which subsequently occurred on September 8, 2017, the date on which Equifax disclosed the breach to the public.

23. In the public statement informing the public of the massive breach, now – former Chairman and Chief Executive Officer, Richard F. Smith claimed, "We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations."[12] But, the massive breach of both the trust placed in Equifax by millions of consumers and of Equifax's duty to protect the sensitive data it collects belies any assertion of "pride" Equifax has in protecting data. Clearly, Equifax did not do nearly enough to protect the consumer data that it stored and used to make its extraordinary profits. Equifax merely needed to install a patch that was publicly known and available for months. It failed to do so. And, there is no reasonable basis for its decision to keep the massive data breach secret for six weeks, especially while its own executives dumped stock to avoid the inevitable drop in share price.

24. Rather than acknowledge that Equifax, as a whole, failed to adequately protect the sensitive data of over 140 million Americans, former CEO Smith blamed one of the biggest data breaches in history on one person – and it was not himself. In his testimony before Congress, Smith claimed that the breach was the fault of a single Equifax staffer who mishandled the patches,

[12] *Equifax Announces Personnel Changes*, *supra* note 6.

stating that "the individual who is responsible for communicating in the organization to apply the patch, did not."[13]

25. "But breaches are almost never a single person's fault," said Nate Fick, CEO at security firm Endgame.[14] "Often times, it's a lack of accountability and poor security culture building up to the attack, not one person's mistake."[15]

26. Equifax is acutely aware that the consumer and business information it stores is highly sensitive and highly valuable to identity thieves and other criminals. On its website, Equifax states:

> We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax.[16]

27. There is little question that Equifax was aware of the need to protect consumers' highly valuable personal and financial information. Without question, by collecting and storing such extensive and detailed customer data, Equifax created an obligation for itself to use every means available to protect this data from falling into the hands of criminals. Clearly, this obligation would include using the latest and strongest methods to prevent website application exploitation. Yet, that is exactly the type of simplistic attack that led to the massive data breach in this case.

28. In addition to actually securing its data from web application exploitation, by installing publicly available and known critical patches, Equifax could have and should have

---

[13]Simon Sharwood, *Sole Equifax Security Worker at Fault for Failed Patch*, THE REGISTER (Oct. 4, 2017), https://www.theregister.co.uk/2017/10/04/sole_security_worker_at_fault_for_equifax_fail_says_former_ceo/.

[14]Alfred Ng, *Equifax Ex-CEO Blames Breach on One Person and Bad Scanner*, CNET.COM (Oct. 3, 2017), https://www.cnet.com/news/equifax-ex-ceo-blames-breach-on-one-person-and-a-bad-scanner/.

[15]*Id.*

[16]*Privacy*, EQUIFAX, http://www.equifax.com/privacy/ (last visited Nov. 08, 2017).

converted consumers' sensitive information into code that would not be immediately identifiable or useful to cyber-thieves. Yet Equifax apparently did not even take that step. It stored consumers' most sensitive information, including Social Security numbers, birth dates, drivers' license numbers and other credit information in plain text, readily identifiable and usable by anyone.

29. Because Equifax allowed criminals to obtain such varied and sensitive personal data about each affected individual, there is little doubt that these victims will suffer significant and persistent financial harm as a result. "It's one of the worst hacks imaginable," said Dan Guido, CEO of the cyber-security firm Trail of Bits.[17] "People should be extraordinarily angry at companies like Equifax. We place a huge amount of trust in them about money matters but they're so easily compromised by simplistic attacks like this one."[18] "This cyber-attack was so big, and it contained so much highly sensitive information, that it's going to linger for a long time. Consumers need to keep their guards up for the foreseeable future."[19]

30. As a result of Equifax's inadequate data security, criminals now possess the personal and financial information of the Plaintiffs and tens of millions of other Americans. Unlike credit card data breaches, like those recently at Target Corp. and Home Depot, the harm here cannot be attenuated by cancelling and reissuing credit cards. Thieves who obtained consumers' personal information by hacking into Equifax's systems could use an individual's social security number to apply for credit in that person's name, then verify their phone identity with the Equifax historic information. In addition, the thieves could use the date to open up fraudulent financial

[17]Allen St. John, *Equifax Data Breach: What Consumers Need to Know*, CONSUMER REPORTS, https://www.consumerreports.org/privacy/what-consumers-need-to-know-about-the-equifax-data-breach/ (last updated Sept. 21, 2017).
[18]*Id.*
[19]Jessica Dickler, *Despite Attention from Equifax Brach, Consumers Doing Little to Protect Themselves*, CNBC.COM (Oct. 11, 2017), https://www.cnbc.com/2017/10/11/despite-equifax-breach-consumers-doing-little-to-guard-against-fraud.html.

accounts, sell the stolen data to other criminals on the black market, and otherwise gain millions of dollars through fraud that victims will not be able to detect until it is too late. Consumers victimized by the breach may have their credit profiles destroyed, causing them to lose the ability to borrow money, obtain credit, or even open bank accounts.

31. A black market exists in which criminals openly buy and sell personal information. "A stolen credit card alone is worth $1 in the black market," Justin Lie, CEO of global online fraud management company CashShield, told FOX Business.[20] "This number multiplies 5x with each added associated piece of information to that credit card number."[21] A stolen credit card with a home address is worth $5, the addition of an email address increases the value to $25, and so on.

32. But this breach is far more valuable. The data breach consists of over 143 million records that include name, address, birthdate, SSN, drivers' license numbers, employment information, and even income. Complete identity records like those at issue here can sell for up to $250-$400 on the black market, making this a breach potentially worth in excess of $500 billion to cybercriminals.[22] "Hackers stand to profit substantially off of the Equifax case because unlike a normal hack, which generally compromises a single piece of personal data per individual, the Equifax hack gave thieves access to an entire correlated set of data points for each victim."[23]

33. In addition, criminals can file false federal and state tax returns in victims' names, preventing or at least delaying their receipt of legitimate tax refunds and potentially making

---

[20]Brittany De Lea, *Equifax Hack: How Much Your Stolen Info is Worth on Black Market*, FOX BUSINESS (Sept. 12, 2017), http://www.foxbusiness.com/markets/2017/09/12/equifax-hack-how-much-your-stolen-info-is-worth-on-black-market.html.

[21]*Id.*

[22]*See 2016 Underground Hacker Marketplace Report*, SECUREWORKS.COM, http://www.secureworks.com/assets/pdf-store/white-papers/wp-underground-hacking-report.pdf (last visited Nov. 7, 2017).

[23]De Lea, *supra* note 20.

victims targets of IRS and state tax investigations. The potential harm does not stop there. If a thief takes out a prescription in a victim's name, that will go on the victim's medical record, potentially interfering with the victim's ability to receive medical treatment or obtain prescriptions necessary for the victim but that counteract with the prescription obtained by the criminal.[24] According to Eva Velasquez, CEO of Identity Theft Resource Center, a nonprofit that assists thousands of identity fraud victims annually, more sinister criminals could use stolen data to assume victims' identities and pin crimes on them. "If someone gets a driver's license in your name and runs a red light or gets a speeding ticket, you're on the hook," says Velasquez. "The criminal's not going to pay it -- and soon enough there could be a warrant out for your arrest."[25] There have even been instances where fraud victims discovered that prisoners were serving sentences in their names.[26]

34. To afford themselves some modicum of protection, persons affected by the breach must add themselves to credit fraud watch. However, that in turn substantially impairs their ability to obtain additional credit. Many experts advise a flat out freeze on all credit accounts, making it impossible to rent a car, obtain student loans, or buy or rent furniture, a new TV, or complete major purchases like buying a new car or home.

35. To make any and every credit-based purchase or rental, each individual will have to take the time to request that the freeze be suspended, wait days for suspension to occur, and then reinstate the freeze, every single time the individual wants to make a purchase or rental for the foreseeable future. Furthermore, because there are three major credit bureaus, consumers will likely need to take these steps with all of them because they will not know which bureau a creditor

[24]David Goldman, *Equifax Hack: What's the Worst that Can Happen?*, CNN.COM (Sept. 11, 2017), http://money.cnn.com/2017/09/11/technology/equifax-identity-theft/index.html.
[25]*Id.*
[26]*See id.*

may consult. Also, credit freezes often cost the consumer money, saddling consumers with even more costs as a result of Equifax's failure to protect consumers' data.

36. Although Equifax is offering free credit monitoring to some customers, the credit monitoring services do little to prevent wholesale identity theft. Experts warn that batches of stolen information will not be immediately dumped on the black market. "[O]ne year of credit monitoring may not be enough. Hackers tend to lay low when data breaches are exposed. . .They often wait until consumers are less likely to be on the lookout for fraudulent activities."[27] In light of the seriousness of this breach and the nature of the data involved, one year of credit monitoring is certainly insufficient.

37. This is especially true given the hackers' theft of SSNs, which unlike credit cards, are not reissued. A cybercriminal, especially one with millions of SSN records, can hold on to stolen information for years until the news of the theft has subsided, then steal a victim's identity, credit, and bank accounts, resulting in thousands of dollars in losses and lost time and productivity. Thus, Plaintiffs and the Class must take additional steps to protect their identities and bear the burden and expense of identity and credit monitoring for years – even decades – to come.

38. Sadly, this is not the first time Equifax has failed to prevent a data breach. Earlier this year, Equifax's computer security was breached on two separate occasions. First, Equifax disclosed that its TALX payroll division was hacked. As reported by Brian Krebs, "[i]dentity thieves who specialize in tax refund fraud had big help this past tax year from Equifax, one of the nation's largest consumer data brokers and credit bureaus. . . . Equifax says crooks were able to

[27]AnnaMaria Andriotis, *Into the Breach: Identity-Theft Protection*, THE WALL STREET JOURNAL (Jan. 24, 2015), https://www.wsj.com/articles/into-the-breach-identitytheft-protection-1390607608.

reset the 4-digit PIN given to customer employees as a password and then steal W-2 tax data after successfully answering personal questions about those employees."[28]

39. Equifax admitted unauthorized access to customers' employee tax records happened between April 17, 2016 and March 29, 2017.[29] For over a year Equifax's customers' employees' data was being stolen—and Equifax apparently had no idea, or at least did nothing to stop it.

40. Security experts publicly told Equifax that it was not doing enough:

> Generally. Forensically. Exactly. Potentially. Actually. Lots of hand-waving from the TALX/Equifax suits. But Equifax should have known better than to rely on a simple PIN for a password, says Avivah Litan, a fraud analyst with Gartner Inc.
>
> "That's so 1990s," Litan said. "It's pretty unbelievable that a company like Equifax would only protect such sensitive data with just a PIN.
>
> Litan said TALX should have required customers to use stronger two-factor authentication options, such as one-time tokens sent to an email address or mobile device (as Equifax now says TALX is doing — at least with those we know were notified about possible employee account abuse).[30]

41. Second, on September 18, 2017, Equifax disclosed a separate data breach in March 2017 that it claims was unrelated to the breach that led to its loss of account information for 143 million Americans.[31] While Equifax provided little detail of this prior data breach, it disclosed that it hired FireEye, Inc.'s Mandiant investigations group upon discovery of suspicious network activity. That investigation was apparently concluded without discovery of

---

[28] *See* Brian Krebs, *Fraudsters Exploited Lax Security at Equifax's TALX Payroll Division*, KREBS ON SECURITY (May 18, 2017), https://krebsonsecurity.com/2017/05/fraudsters-exploited-lax-security-at-equifaxs-talx-payroll-division/.
[29] *See id.*
[30] *See id.*
[31] Robert McMillan & AnnaMaria Andriotis, *Equifax Discloses Earlier Cybersecurity Incident, But No* Details, THE WALL STREET JOURNAL, https://www.wsj.com/articles/equifax-discloses-earlier-cybersecurity-incident-but-no-details-1505786212 (last updated Sept. 19, 2017).

the vulnerability leading to the massive breach which Equifax admits began in May 2017. Equifax re-hired Mandiant in response to the massive, most recent breach.[32]

42. Quite obviously, Equifax did not learn from its mistakes. It followed its negligent protection of employee data at its TALX subsidiary, and negligent protection of its systems as evident from the March 2017 data breach, with negligent protection of the personal and financial information of nearly half the adult population of the United States. It ignored public warnings about a specific threat and public indications that the threat was being widely exploited by hackers. It had unfettered access and ample time to install a patch in an effective manner that would have prevented this catastrophe for 143 million consumers. But it did not do it. As a result, "criminals" have stolen consumers names, Social Security numbers, birthdates, driver's license numbers, addresses, and in some cases credit history and credit card numbers.

IV. CLASS ACTION ALLEGATIONS

43. Plaintiffs bring this action against the Defendant pursuant to Rules 23(a), (b)(2), and (b)(3), of the Federal Rules of Civil Procedure, on behalf of themselves and all other persons and entities similarly situated. Plaintiffs seek certification of the following classes (referred to collectively as the "Class"):

The Nationwide Class

All persons in the United States whose personal and financial information was compromised as a result of the data breach first disclosed by Equifax on or about September 7, 2017.

The Florida Subclass

All persons in Florida whose personal and financial information was compromised as a result of the data breach first disclosed by Equifax on or about September 7, 2017.

[32] *See id.*

The California Subclass

All persons in California whose personal and financial information was compromised as a result of the data breach first disclosed by Equifax on or about September 7, 2017.

A. Numerosity

44. The individual Class Members are so numerous that joinder of all members in a single action is impracticable. Equifax has admitted that the records of 145.5 million individuals were breached. This number has been confirmed by a third-party cyber security firm who conducted an analysis of the number of individuals potentially impacted.[33] Thus, the Nationwide Class consists of tens of millions of individuals whose personal and financial information was compromised as result of the breach of Equifax's data systems. The Florida Subclass consists of tens of thousands of individuals whose personal and financial information was compromised as result of the breach of Equifax's data systems. Finally, the California Subclass consists of tens of thousands of whose personal and financial information was compromised as result of the breach of Equifax's data systems.

45. The names and addresses of individual Class Members can be identified in the records maintained by Equifax. Indeed, the fact that Equifax possessed this information and more without adequately protecting it is the very basis of this lawsuit. Equifax has already announced that it will send written notice by mail to every individual who was impacted by the data breach, indicating that all Class Members can be identified. The Plaintiffs do not anticipate any difficulties in the management of this action as a class action.

[33] *Equifax Announces Cybersecurity Firm has Concluded Investigation*, *supra* note 5.

B. Commonality

46. There are questions of law and fact that are common to the claims of the Plaintiffs and the Class. These common questions predominate over any questions that are particular to any individual Class Member. Among such common questions of law and fact are the following:

a. Whether Equifax engaged in the wrongful conduct alleged herein;

b. Whether Equifax's conduct was deceptive, unfair, and/or unlawful;

c. Whether Equifax owed a duty to the Plaintiffs and members of the Class to adequately protect their personal and financial information,

d. Whether Equifax used reasonable and industry-standard measures to protect Class Members' personal and financial information;

e. Whether Equifax knew or should have known that its data system was vulnerable to attack;

f. Whether Equifax's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of tens of millions of Class Members' personal and financial data;

g. Whether Equifax should have notified the public immediately after it learned of the breach;

h. Whether Equifax violated state statutory consumer protection, consumer fraud, data-breach-notification, and other applicable laws;

i. Whether Equifax violated state common law regarding negligence or otherwise Florida common law;

j. Whether Plaintiffs and the Class Members are entitled to recover actual damages, statutory damages, and/or punitive damages; and

k. Whether Plaintiffs and Class Members are entitled to restitution, disgorgement, and/or other equitable relief.

C. Typicality

47. The Plaintiffs' claims are typical of the claims of the Class because all members of the Class were injured through the same misconduct by Equifax. Plaintiffs, like all Class Members, were damaged by Equifax's misconduct as alleged above, resulting in the breach of Equifax's data systems and the theft of the Plaintiffs' and the Class Members' personal and financial information.

D. Adequacy of Representation

48. The Plaintiffs are adequate representatives of the Class and will fairly and adequately protect the interests of the Class. Plaintiffs are committed to the vigorous prosecution of this action and have retained competent counsel, experienced in litigation of this nature, to represent them. There is no hostility between the Plaintiff and the unnamed Class Members. Plaintiffs anticipate no difficulty in the management of this litigation as a class action.

49. To prosecute this action, Plaintiffs have chosen the law firm of Buckner + Miles. This firm is experienced in class action litigation and has the financial and legal resources to meet the substantial costs and legal issues associated with this type of litigation.

E. Requirements of Fed. R. Civ. P. 23(b)(3)

1. Predominance

50. The questions of law or fact common to the claims of the Plaintiffs and the Class predominate over any questions of law or fact affecting only individual members of the Class. All claims by the Plaintiffs and the unnamed Class Members are based on the Defendant's misconduct with respect to the personal and financial information contained in Equifax's data systems,

resulting in the breach of those data systems and the theft of the Plaintiffs' and the Class Members' personal and financial information

51. Common issues predominate when, as here, liability can be determined on a class-wide basis.

52. As a result, when determining whether common questions predominate, courts focus on the liability issue, and if the liability issue is common to the class, as it is in this case, common questions will be held to predominate over individual questions.

53. Because all claims by Plaintiff and the unnamed Class members are based on the same misconduct by the Defendant, the predominance requirement of Fed. R. Civ. P. 23(b)(3) is satisfied.

2. Superiority

54. A class action is superior to tens of millions of individual actions in part because of the non-exhaustive factors listed below:

a. Joinder of all Class Members would create extreme hardship and inconvenience because of their geographical dispersion. Class Members reside throughout the United States.

b. Individual claims by the Class Members are impractical because the costs to pursue individual claims exceed the value of what any one Class Member has at stake. The Defendant is large and well-funded. As a result, individual Class members are unable to prosecute and control separate actions.

c. The interests of justice will be well served by resolving the common disputes of potential Class Members in one forum.

d. The action is manageable as a class action; individual lawsuits are not economically maintainable as individual actions.

V. COUNTS

COUNT I
NEGLIGENCE
(ON BEHALF OF THE NATIONWIDE CLASS)

55. Plaintiffs reallege and incorporate paragraphs 1 through 54 above, as if fully set forth herein.

56. By collecting and storing the sensitive personal and financial information belonging to the Plaintiffs and the members of the Nationwide Class and State Subclasses, including highly sensitive information such as Social Security numbers, driver's license numbers, dates of birth, street addresses and financial account information, Equifax assumed a duty to the Plaintiffs and the members of the Nationwide Class and State Subclasses to use reasonable and/or industry standard care to secure that information against theft and misuse.

57. Equifax breached that duty by, *inter alia*:

a. Failing to detect a breach in its systems when it first occurred;

b. Failing to seal the breach in its systems when it first occurred;

c. Failing to timely detect any flaws or vulnerabilities in its systems, including the Apache Struts Web Application;

d. Failing to timely and/or properly patch and repair its systems, including the Apache Struts Web Application;

e. Failing to comply with industry-standard security practices;

f. Failing to implement adequate security systems to protect the personal and financial information contained in its systems;

g. Failing to encrypt the sensitive personal and financial information in its systems so as not to be readily readable by hackers; and

h. Failing to promptly, timely, and accurately, inform Plaintiffs and the Class that their personal and financial information had been stolen.

58. As a direct and proximate result of Equifax's failure to use reasonable and/or industry-standard care to protect the personal and financial information it collected and stored on its systems, the personal and financial information of the Plaintiffs and the members of the Nationwide Class and State Subclasses were stolen, resulting in damages to the Plaintiffs and the members of the Nationwide Class and State Subclasses, including, but not limited to: identity theft; the loss of the monetary value, including the market value, of their personal and financial information; damage to credit scores and credit reports; and time and expense related to: (a) finding fraudulent accounts; (b) monitoring their identity; (c) credit monitoring and identity theft prevention; (d) freezing access to their credit reports at major credit bureaus; (e) income tax refund fraud and the potential for income tax refund fraud; (f) the general nuisance and annoyance of dealing with all these issues resulting from the data breach; and (g) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the data breach.

WHEREFORE, Plaintiffs, on behalf of themselves and all similarly situated individuals and entities, demand judgment against Equifax for compensatory damages, pre- and post-judgment interest, attorneys' fees, costs incurred in bringing this action, and any other relief this Court deems just and proper.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF THE NATIONWIDE CLASS)

59. Plaintiffs reallege and incorporate paragraphs 1 through 54 above, as if fully set forth herein.

60. Section 5 of the Federal Trade Commission Act (the "FTC Act"), otherwise known as 15 U.S.C. § 45, prohibits "unfair or deceptive acts or practices in or affecting commerce . . . ." Under the FTC Act, an act or practice may be found to be unfair where it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."

61. Equifax committed one or more unfair acts, thereby violating the FTC Act by, *inter alia*:

a. Failing to detect a breach in its systems when it first occurred;

b. Failing to seal the breach in its systems when it first occurred;

c. Failing to timely detect any flaws or vulnerabilities in its systems, including the Apache Struts Web Application;

d. Failing to timely and/or properly patch and repair its systems, including the Apache Struts Web Application;

e. Failing to comply with industry-standard security practices;

f. Failing to implement adequate security systems to protect the personal and financial information contained in its systems;

g. Failing to encrypt the sensitive personal and financial information in its systems so as not to be readily readable by hackers; and

h. Failing to promptly, timely, and accurately, inform Plaintiffs and the Class that their personal and financial information had been stolen.

62. These acts caused or are likely to cause substantial injury to consumers, including, among other things, identity theft, the loss of the monetary value, including the market value, of their personal and financial information, damage to credit scores and credit reports, opening of fraudulent accounts, and income tax refund fraud.

63. The injury caused by Equifax's acts could not be reasonably avoided by consumers as consumers had no control over Equifax's collection of consumers' personal and financial data, the methods by which Equifax stored and protected that data, and the failure by Equifax to timely disclose that its systems were breached, allowing hackers to steal consumers' data.

64. Equifax's unfair acts in violation of the FTC Act as set forth above are not outweighed by countervailing benefits to consumers or competition as Equifax's acts did not, and do not, confer any benefits to consumers or competition.

65. Equifax's failure to comply with the FTC Act constitutes negligence *per se*.

66. Plaintiffs and the Class have suffered injuries in fact, including but not limited to monetary damages, and will continue to be injured and incur damages as a result of Equifax's negligence *per se*.

67. As a direct and proximate result of Equifax's negligence *per se*, the personal and financial information of the Plaintiffs and the members of the Nationwide Class and State Subclasses were stolen, resulting in damages to the Plaintiffs and the members of the Nationwide Class and State Subclasses, including, but not limited to: identity theft; the loss of the monetary value, including the market value, of their personal and financial information; damage to credit scores and credit reports; and time and expense related to: (a) finding fraudulent accounts; (b)

monitoring their identity; (c) credit monitoring and identity theft prevention; (d) freezing access to their credit reports at major credit bureaus; (e) income tax refund fraud and the potential for income tax refund fraud; (f) the general nuisance and annoyance of dealing with all these issues resulting from the data breach; and (g) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the data breach.

WHEREFORE, Plaintiffs, on behalf of themselves and all similarly situated individuals and entities, demand judgment against Equifax for compensatory damages, pre- and post-judgment interest, attorneys' fees, costs incurred in bringing this action, and any other relief this Court deems just and proper.

COUNT III
VIOLATION OF FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
(ON BEHALF OF THE FLORIDA SUBCLASS)

68. Plaintiffs reallege and incorporate paragraphs 1 through 54 above, as if fully set forth herein.

69. This Count is brought pursuant to the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA").

70. At all material times, Plaintiff Tosco and all members of the Florida Subclass were consumers within the meaning of § 501.203, Fla. Stat. (2017), and are entitled to relief under FDUTPA in accordance with § 501.211, Fla. Stat. (2001). At all material times, Equifax conducted trade and commerce within the meaning of § 501.203.

71. Under § 501.204, Fla. Stat. (2017), unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce is prohibited.

72. Equifax has engaged in unfair and deceptive acts and practices as alleged above, including:

a. misrepresenting to the Florida Subclass that it would maintain adequate data privacy and security practices and procedures to safeguard the Florida Subclass Members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. misrepresenting to the Florida Subclass that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Florida Subclass Members' personal and financial information;

c. failing to protect the Florida Subclass Members' personal and financial information from unauthorized disclosure;

d. omitting and concealing the inadequacy of the privacy and security protections in place for the Florida Subclass Members' personal and financial information, with the intent that others rely on the omission and concealment;

e. failing to disclose the data breach to the Florida Subclass Members in a timely and accurate manner; and

f. failing to take proper action following the data breach to enact adequate privacy and security measures to protect Florida Subclass Members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

73. Equifax's unfair and deceptive acts and practices violated duties imposed by the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (2011). Equifax also committed unfair acts as set forth in the FTC Act and under the standards of unfairness and deception as interpreted by the Federal Trade Commission and federal courts.

74. Equifax committed its unfair and deceptive acts and practices in connection with Equifax's trade and commerce in Florida.

75. Equifax's unfair and deceptive acts and practices violated FDUTPA, §§ 501.201 and 501.211.

76. As a direct and proximate result of Equifax's FDUTPA violations, Plaintiff Tosco and the Florida Subclass have been damaged in an amount to be proven at trial.

77. Plaintiff Tosco and the Florida Subclass are entitled to actual damages, attorneys' fees and costs, and all other remedies available under FDUTPA.

WHEREFORE, Plaintiffs, on behalf of themselves and all similarly situated individuals and entities, demand judgment against Equifax for compensatory damages, pre- and post-judgment interest, attorneys' fees, costs incurred in bringing this action, and any other relief this Court deems just and proper.

COUNT IV
VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW
(ON BEHALF OF THE CALIFORNIA SUBCLASS)

78. Plaintiffs reallege and incorporate paragraphs 1 through 54 above, as if fully set forth herein.

79. This Count is brought pursuant to California's Unfair Business Practices Act, CAL. BUS. & PROF. CODE §§ 17200–17210 (1992).

80. At all material times, Plaintiff Ashley and the members of the California Subclass were persons within the meaning of CAL. BUS. & PROF. CODE § 17201 (1977), and are entitled to relief under the act in accordance with § 17204 (2009).

81. At all material times, Equifax operated in California and engaged in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constituted acts of "unfair competition" within the meaning of CAL. BUS. & PROF. CODE § 17200 by, among other things:

a. representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard California Subclass members' personal and financial information from unauthorized disclosure, release, data breaches, and theft; and representing and advertising that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of California Subclass Members' personal and financial information, but failing to do so;

b. establishing the sub-standard security practices and procedures described above;

c. soliciting and collecting California Subclass Members' personal and financial information with knowledge that the information would not be adequately protected;

d. storing California Subclass Members' personal and financial information in an unsecure electronic environment;

e. failing to disclose the data breach to California Subclass Members in a timely and accurate manner, contrary to the duties imposed by CAL. CIV. CODE § 1798.82 (2017); and

f. failing to take proper action following the data breach to enact adequate privacy and security measures and protect California Subclass Members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

82. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff Ashley and California Subclass Members. Equifax's practice was also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws including the FTC Act, the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (2011), and California's data breach statute, CAL. CIV. CODE § 1798.81.5 (2016). The harm these practices caused to Plaintiff Ashley and the California Subclass members outweighed their utility, if any.

83. Equifax knew or should have known that its computer systems and data security practices were inadequate to safeguard California Subclass Members' personal and financial data, and that the risk of a data breach or theft was highly likely. Equifax's unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Subclass.

84. As a direct and proximate result of Equifax's acts of unfair and unlawful practices, Plaintiff Ashley and the California Subclass were injured and lost money or property. In addition, Plaintiff Ashley and the California Subclass lost their legally protected interest in the

confidentiality and privacy of their personal and financial information, and additional losses described above.

85. Plaintiff Ashley and the California Subclass are entitled to restitution, disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices, declaratory relief, and all other remedies available under California's Unfair Business Practices Act, as well as attorney's fees and costs pursuant to CAL. CIV. PROC. CODE. §1021.5.

WHEREFORE, Plaintiffs, on behalf of themselves and all similarly situated individuals and entities, demand judgment against Equifax for compensatory damages, pre- and post-judgment interest, attorneys' fees, costs incurred in bringing this action, and any other relief this Court deems just and proper.

COUNT V
VIOLATION OF THE CALIFORNIA DATA BREACH ACT
(ON BEHALF OF THE CALIFORNIA SUBCLASS)

86. Plaintiffs reallege and incorporate paragraphs 1 through 54 above, as if fully set forth herein.

87. This Count is brought pursuant to the California Data Breach Act, CAL. CIV. CODE. §§ 1798.80–1798.84.

88. At all material times, Plaintiff Ashley was a resident of California.

89. CAL. CIV. CODE § 1798.82 (2017), requires:

> (a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security

> credential could render that personal information readable or useable. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
>
> (b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

90. Under § 1798.82, the notification must include:

> (A) The name and contact information of the reporting person or business subject to this section.
> (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
> (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.
> (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
> (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
> (F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

91. The breach of Equifax's systems as alleged above constituted a breach of the security system of Equifax within the meaning of § 1798.82(g) of the California Data Breach Act.

92. Plaintiff Ashley and the California Subclass Members' names, addresses, email addresses, birthdates, social security numbers, employment and income information constitute personal information as set forth in § 1798.82(i) of the California Data Breach Act.

93. Equifax unreasonably delayed in informing Plaintiff Ashely and the members of the California Subclass about the breach of security of their confidential and non-public information after Equifax knew the data breach occurred.

94. Equifax failed to disclose to Plaintiff Ashley and the California Subclass, without unreasonable delay and in the most expedient time possible as required by the California Data Breach Act, the breach of security of consumers' personal and financial information when they knew or reasonably believed such information had been compromised.

95. Equifax's conduct in failing to timely disclose the breach of the security system of Equifax was willful, intentional, and/or reckless as Equifax detected the breach on July 29, 2017, yet chose not to disclose it to the public until September 7, 2017.

96. Equifax's conduct violated the California Data Breach Act.

97. As a direct and proximate result of Equifax's violations of the act, Plaintiff Ashley and the California Subclass have been damaged in an amount to be proven at trial.

98. Plaintiff Ashley and the California Subclass are entitled actual damages, statutory damages for Equifax's willful, intentional and/or reckless violation of § 1798.82, and all other remedies available under California's Data Breach Act, as well as attorney's fees and costs pursuant to CAL. CIV. PROC. CODE. §1021.5.

WHEREFORE, Plaintiffs, on behalf of themselves and all similarly situated individuals and entities, demand judgment against Equifax for compensatory damages, pre- and post-judgment interest, attorneys' fees, costs incurred in bringing this action, and any other relief this Court deems just and proper.

COUNT VI
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT
(ON BEHALF OF THE NATIONWIDE CLASS)

99. Plaintiffs reallege and incorporate paragraphs 1 through 54 above, as if fully set forth herein.

100. This Count is brought pursuant to the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681a–1681x (2011).

101. At all material times, Plaintiffs and the Class were consumers within the meaning of 15 U.S.C. § 1681a (2011), and are entitled to relief under 15 U.S.C. § 1681n (2008).

102. Equifax is a consumer reporting agency as set forth in § 1681a(f) of the FRCA because, for monetary fees, dues, or on a noncooperative basis, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

103. Under § 1681a(d), "consumer report" means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for, among other things, credit or insurance to be used primarily for personal, family, or household purposes, or for employment purposes.

104. 15 U.S.C. § 1681e (2010), requires consumer reporting agencies, like Equifax, to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b. Pursuant to § 1681b (2015), Equifax may only furnish consumer reports under the circumstances listed within that section, "and no other."

105. None of the enumerated purposes listed under § 1681b permitted Equifax to furnish consumer reports to unauthorized or unknown entities, or to entities who obtained the Class' personal and financial data by breaching Equifax's data systems.

106. Equifax furnished the Class Members' consumer reports by:

a. disclosing consumer reports to unauthorized entities and computer hackers;

b. allowing unauthorized entities and computer hackers to access consumer reports stored in Equifax's systems;

c. knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports; and

d. knowingly and/or recklessly failing to patch and/or repair vulnerabilities in its data systems that would prevent unauthorized entities from accessing their consumer reports.

107. Equifax willfully and/or recklessly violated §§ 1681b and 1681e(a) by providing individuals with access to consumer reports for impermissible purposes and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under § 1681b of the FCRA. The willful and reckless nature of Equifax's violations is supported by, among other things, Equifax's numerous data breaches in the past. Furthermore, Equifax, as an entity that promotes itself as a leader in data breach security and prevention, was well aware of the importance of the measures organizations should take to prevent data breaches, yet willingly failed to take them.

108. Equifax also acted willfully and recklessly because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. Despite knowing of these legal obligations, Equifax acted consciously in failing to maintain reasonable security measures, thereby providing a means for unauthorized intruders to obtain and misuse Plaintiffs' and the Class' personal information for no permissible purposes under the FCRA.

109. As a direct and proximate result of Equifax's willful violation of the FCRA, Plaintiffs and the Class have been damaged in an amount to be proven at trial.

110. Plaintiffs and each member of the Class are entitled to recover any actual damages sustained by him or her or damages of not less than $100 and not more than $1,000, as well as punitive damages, costs of the action and reasonable attorneys' fees pursuant to 15 U.S.C. § 1681n (2008).

WHEREFORE, Plaintiffs, on behalf of themselves and all similarly situated individuals and entities, demand judgment against Equifax for compensatory damages, pre- and post-judgment interest, attorneys' fees, costs incurred in bringing this action, and any other relief this Court deems just and proper.

COUNT VII
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT
(ON BEHALF OF THE NATIONWIDE CLASS)

111. Plaintiffs reallege and incorporate paragraphs 1 through 54 above, as if fully set forth herein.

112. This Count is brought pursuant to the FCRA.

113. At all material times, Plaintiffs and the Class were consumers within the meaning of 15 U.S.C. § 1681a, and are entitled to relief under 15 U.S.C. § 1681n.

114. Equifax is a consumer reporting agency as set forth in § 1681a(f) of the FRCA because, for monetary fees, dues, or on a noncooperative basis, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

115. Under § 1681a(d), "consumer report" means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit

worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for, among other things, credit or insurance to be used primarily for personal, family, or household purposes, or for employment purposes.

116. 15 U.S.C. § 1681e requires consumer reporting agencies, like Equifax, to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b. Pursuant to § 1681b, Equifax may only furnish consumer reports under the circumstances listed within that section, "and no other."

117. Thus, under the FRCA, Equifax had a duty to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under §1681b, "and no other."

118. Equifax breached that duty by, *inter alia*:

a. Failing to take security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports;

b. Failing to detect a breach in its systems when it first occurred;

c. Failing to seal the breach in its systems when it first occurred;

d. Failing to timely detect any flaws or vulnerabilities in its systems, including the Apache Struts Web Application;

e. Failing to timely and/or properly patch and repair its systems, including the Apache Struts Web Application;

f. Failing to comply with industry-standard security practices;

g. Failing to implement adequate reasonable security systems to protect the personal and financial information contained in its systems;

h. Failing to encrypt the sensitive personal and financial information in its systems so as not to be readily readable by hackers;

119. Equifax's negligent conduct violated §§ 1681b and 1681e(a) and resulted in unauthorized individuals accessing consumer reports for impermissible purposes.

120. As a direct and proximate result of Equifax's conduct, Plaintiffs and the Class have been damaged in an amount to be proven at trial.

121. Plaintiffs and each member of the Class are entitled to recover any actual damages sustained by him or her, as well as costs of the action and reasonable attorneys' fees pursuant to 15 U.S.C. § 1681o (2004).

WHEREFORE, Plaintiffs, on behalf of themselves and all similarly situated individuals and entities, demand judgment against Equifax for compensatory damages, pre- and post-judgment interest, attorneys' fees, costs incurred in bringing this action, and any other relief this Court deems just and proper.

RELIEF REQUESTED

Plaintiffs respectfully request that this Court:

A. Certify this action as a class action under Federal Rule of Civil Procedure 23(a) and (b)(3); appoint Plaintiffs as the representatives of the Nationwide Class, Plaintiff Tosco representative of the Florida Subclass, and Plaintiff Ashley representative of the California Subclass; and appoint Buckner + Miles as Class Counsel.

B. Award Plaintiffs and the Class all common law, compensatory, and special damages as well as restitution and statutory remedies for Equifax's violations of law, including pre- and post-judgment interest on these amounts.

C. Award Plaintiffs and the Class punitive damages.

D. Award Plaintiffs and the Class their attorneys' fees, costs, and expenses.

E. Award Plaintiffs and the Class such further relief as is appropriate in the interests of justice.

DEMAND FOR JURY TRIAL

Plaintiffs request a jury trial on any and all counts for which trial by jury is permitted by law.

Dated: November 9, 2017.

Respectfully submitted,

s/David M. Buckner
David M. Buckner (Florida Bar No. 60550)
david@bucknermiles.com
Seth Miles, Esq. (Florida Bar No. 0385530)
seth@bucknermiles.com
Brett E. von Borke (Florida Bar No. 0044802)
vonborke@bucknermiles.com
Guy Kamealoha Noa (Florida Bar No. 111148)
noa@bucknermiles.com
Buckner + Miles
3350 Mary Street
Miami, Florida 33133
Telephone: 305.964.8003
Facsimile: 786.523.0485

Attorneys for Plaintiff

JS 44 (Rev. 2/08)

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 THE REVERSE OF THE FORM.) **NOTICE: Attorneys MUST Indicate All Re-filed Cases Below.**

I. (a) PLAINTIFFS

Chris Tosco, and Mark Ashley, Individually and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff Miami-Dade
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorney's (Firm Name, Address, and Telephone Number)

Buckner + Miles
3350 Mary Street, Miami, FL 33133
305.964.8003

DEFENDANTS

Equifax Inc.

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

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

Attorneys (If Known)

(d) Check County Where Action Arose: ☑ MIAMI- DADE ☐ MONROE ☐ BROWARD ☐ PALM BEACH ☐ MARTIN ☐ ST. LUCIE ☐ INDIAN RIVER ☐ OKEECHOBEE ☐ HIGHLANDS

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)

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 (Excl. 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

PERSONAL INJURY
- ☐ 362 Personal Injury - Med. Malpractice
- ☐ 365 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
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 444 Welfare
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 440 Other Civil Rights

PRISONER PETITIONS
- ☐ 510 Motions to Vacate Sentence

Habeas Corpus:
- ☐ 530 General
- ☐ 535 Death Penalty
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition

FORFEITURE/PENALTY
- ☐ 610 Agriculture
- ☐ 620 Other Food & Drug
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 630 Liquor Laws
- ☐ 640 R.R. & Truck
- ☐ 650 Airline Regs.
- ☐ 660 Occupational Safety/Health
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Mgmt. Relations
- ☐ 730 Labor/Mgmt.Reporting & Disclosure Act
- ☐ 740 Railway Labor Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Empl. Ret. Inc. Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 463 Habeas Corpus-Alien Detainee
- ☐ 465 Other Immigration Actions

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

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 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
- ☐ 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
- ☐ 810 Selective Service
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 875 Customer Challenge 12 USC 3410
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 892 Economic Stabilization Act
- ☐ 893 Environmental Matters
- ☐ 894 Energy Allocation Act
- ☐ 895 Freedom of Information Act
- ☐ 900 Appeal of Fee Determination Under Equal Access to Justice
- ☐ 950 Constitutionality of State Statutes

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

☑ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Re-filed- (see VI below) ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district (specify) ☐ 6 Multidistrict Litigation ☐ 7 Appeal to District Judge from Magistrate Judgment

VI. RELATED/RE-FILED CASE(S).

(See instructions second page): a) Re-filed Case ☐ YES ☑ NO b) Related Cases ☐ YES ☑ NO

JUDGE DOCKET NUMBER

VII. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing and Write a Brief Statement of Cause **(Do not cite jurisdictional statutes unless diversity)**:

28 U.S.C. § 1332(d)(2)(A)

LENGTH OF TRIAL via _____ days estimated (for both sides to try entire case)

VIII. REQUESTED IN COMPLAINT:

☑ CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23

DEMAND $

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

ABOVE INFORMATION IS TRUE & CORRECT TO THE BEST OF MY KNOWLEDGE

SIGNATURE OF ATTORNEY OF RECORD

DATE
November 9, 2017

FOR OFFICE USE ONLY

AMOUNT _____ RECEIPT # _____ IFP _____

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Southern District of Florida

Chris Tosco, and Mark Ashley, Individually and on behalf of all others similarly situated,

Plaintiff(s)

v.

Equifax Inc.

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Equifax Inc.
c/o Registered Agent: Shawn Baldwin
1550 Peachtree Street, N.W.
Fulton, Georgia 30309-2402

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

David M. Buckner, Esq.
Buckner + Miles
3350 Mary Street
Miami, Florida 33133

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: