UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MARIO VICE, Individually and on Behalf of All Others Similarly situated, Plaintiff, vs. EQUIFAX INC., a Delaware corporation, Defendant.	Civil Action No. CLASS ACTION COMPLAINT **JURY TRIAL DEMANDED**

COMPLAINT

For his complaint against defendant Equifax Inc. ("Equifax" or "Defendant"), plaintiff Mario Vice ("Plaintiff") alleges, in his own right and on behalf of all other Louisiana residents similarly situated, as follows:

NATURE OF THE ACTION

1. A credit reporting agency must, above all else, protect the highly sensitive personal and financial information that it collects from consumers. When a consumer's information is collected by a credit reporting agency—often without the consent or even the knowledge of the consumer—the credit reporting agency must be at the absolute forefront of data security to ensure that thieves and hackers

could *never* get access to the data the agency has collected. It cannot fail to patch critical software effectively and promptly, especially when fixes are available, and even more so when exploits based on the vulnerability in that software have been widely reported. And when a data breach involving up to 143 million records of innocent consumers occurs, a credit reporting agency must *immediately and accurately* notify all those affected to prevent consumers from becoming victims of identity theft. And it must take immediate steps to mitigate the damages it has caused—not half-steps that could lead to self-enrichment. This lawsuit stems from Equifax's abject failure to follow these simple rules.

FACTUAL BACKGROUND

2. Equifax is one of the big three credit reporting agencies in the U.S.[1] Founded in 1899, it is the oldest of the credit bureaus and claims to maintain information on over 800 million consumers and more than 88 million businesses worldwide. Equifax's stock is listed on the New York Stock Exchange. In its 2016 Annual Report, Equifax claimed operating revenue totaling $3.145 billion and operating income of $818 million.[2]

3. On September 7, 2017, Equifax first disclosed that its computer systems had been hacked. The company stated it is continuing its investigation

[1] Experian and TransUnion are the other two. Innovis is considered a fourth credit reporting agency.

[2] *See* https://investor.equifax.com/~/media/Files/E/Equifax-IR/Annual%20Reports/2016-annual-report.pdf (last accessed Oct. 18, 2017).

into the scope of the breach, but it indicated, "Criminals 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."[3]

4. Equifax admits, "The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. 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]

5. Ironically, Equifax is an agency that scores of consumers use to guard against identity theft, a service Equifax markets and sells. Businesses pay Equifax to verify customers are who they say they are. Robert Siciliano, CEO of IDTheftSecurity.com told NBC News: "Equifax is tasked with actually protecting this information in the form of identity theft protection and here we are with almost half of the country's population being affected."[5]

6. As NBC News further reported: "Even if you don't think you're a customer of Equifax, there's a strong possibility they still have your data. As a

---

[3] *See* Equifax September 7, 2017 press release at: https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628 (last accessed Oct. 16, 2017) ("Equifax Press Release").

[4] *Id.*

[5] *See* https://www.nbcnews.com/tech/security/massive-equifax-data-breach-could-impact-half-u-s-population-n799686 (last accessed Oct. 16, 2017).

credit reporting agency, Equifax gets information from credit card companies, banks, lenders and retailers to help it determine a person's credit score."[6]

7. The massive data breach could have been prevented and should have been detected and disclosed earlier. While Equifax says the intrusion occurred at least as early as "mid-May" 2017, it claims that the breach was first detected on July 29, 2017. Equifax—a company whose business is the collection and storage of extremely sensitive and valuable data—admits its systems were compromised for ten full weeks before it had any idea it had been hacked.

8. But what makes this breach even worse is that it was fully preventable. Equifax had notice of the software vulnerability that allowed this attack on 143 million Americans' data for some *two months* before the breach occurred. In fact, there were press reports of widespread attempts by hackers to exploit this vulnerability. Yet Equifax failed to take the steps necessary to secure its treasure of consumers' personal information—or to seal off *any* outside access to this treasure while it worked on a fix—if it indeed made any effort to do so in response to notice of the vulnerability.

9. In the days following the September 7, 2017 revelation of this breach, there were reports that the breach occurred due to a vulnerability in an open-source

---

[6] *See id.*

web application framework called Apache Struts.[7] At first the surmise was that the vulnerability may have been one announced in early September 2017, and thus new to all.[8] But the Apache Struts Foundation questioned this report given the timing of the announcement of that vulnerability versus Equifax's disclosure that its data storage may have been breached as early as mid-May 2017 (and that it learned of this breach in late July 2017).[9]

10. And now Equifax admits that it was the *March 2017* Apache Struts bug that one or more hackers exploited. In a September 13, 2017 post to its equifaxsecurity2017.com breach-information website, Equifax wrote[10]:

> 1) Updated information on U.S. website application vulnerability. Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638. We continue to work with law enforcement as part of our criminal investigation, and

---

[7] *E.g.*, "Apache Foundation rebuffs allegation it allowed Equifax attack," available at https://www.theregister.co.uk/2017/09/11/apache_rebuts_equifax_allegation/ (last accessed Oct. 16, 2017).

[8] *E.g.*, *id.*

[9] *E.g.*, *id.*; *see also* "The Apache Software Foundation Blog," Sept. 9, 2017, available at https://blogs.apache.org/foundation/entry/apache-struts-statement-on-equifax (last accessed Oct. 16, 2017).

[10] Richard Lawler, "Equifax blames breach on a server flaw it should've patched," Sept. 13, 2017, Engadget, https://www.engadget.com/2017/09/13/equifax-apache-argentina/ (last accessed Oct. 17, 2017).

> have shared indicators of compromise with law enforcement.

11. "Apache Struts CVE-2017-5638" is a critical vulnerability that has been publicly disclosed and widely known since March 2017. In fact, the Apache Software Foundation gave public notice on March 7, 2017,[11] after making a fix freely available on March 6, 2017.[12]

12. And a critical fix it was. Ars Technica reported on March 9, 2017,[13] and March 14, 2017,[14] that sites using this vulnerable software framework were under heavy attack by hackers. As Ars Technica put it, "In a string of attacks that have escalated over the past 48 hours, hackers are actively exploiting a critical vulnerability that allows them to take almost complete control of Web servers used by banks, government agencies, and large Internet companies."[15] The bug was described as "trivial to exploit" and "under attack by hackers who [we]re

---

[11] *See* "Apache Struts Jakarta Multipart Parser File Upload Code Execution Vulnerability," *Cisco*, https://tools.cisco.com/security/center/viewAlert.x?alertId=52972 (last accessed Oct. 18, 2017).

[12] *See, e.g.*, "Critical vulnerability under 'massive' attack imperils high-impact sites [Updated]," *Ars Technica*, Mar. 9, 2017, available at https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/ (last accessed Oct. 18, 2017).

[13] *Id.*

[14] *See, e.g.*, "In-the-wild exploits ramp up against high-impact sites using Apache struts," *Ars Technica*, Mar. 14, 2017, available at https://arstechnica.com/information-technology/2017/03/in-the-wild-exploits-ramp-up-against-high-impact-sites-using-apache-struts/ (last accessed Oct. 18, 2017.

[15] *See* n.12, *supra*.

exploiting it to inject commands of their choice into Struts servers that have yet to install the update," per warnings from researchers.[16] "Making matters worse, at least two working exploits [were] publicly available."[17] In fact, "[e]ight days after developers patched a critical flaw in the Apache Struts Web application framework, there ha[d] been no let-up in the volley of attacks attempting to exploit the vulnerability, which affects a disproportionate number of high-impact websites," according to a security researcher.[18]

13. Yet 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[19] gathered and stored by Equifax, Equifax neglected to take the steps necessary to neutralize the possibility of its systems getting hacked—or to do so effectively in a timely fashion.[20] The result is the massive data breach that is the subject of this complaint, with serious consequences

---

16 *Id.*

17 *Id.*

18 *See* n.14, *supra*.

19 Except where indicated by other specific reference or context, Plaintiff uses the term "personal and financial information" throughout this Complaint also to mean Personal Information (so-called PI) or Personally Identifiable Information (so-called PII).

20 On September 15, 2017, Equifax admitted that it learned of the Apache Struts vulnerability in March 2017 but that whatever steps it took to apply the patch to its systems were ineffective. (*See* Press Release, Equifax, Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes, Sept. 15, 2017).

likely to follow—perhaps for decades—for some 143 million Americans.

14. Shockingly, the entirely preventable Equifax breach was not disclosed for *nearly six weeks* after Equifax's self-delayed discovery. Instead of promptly detecting and promptly notifying the hundreds of millions of consumers whose complete identity information was stolen by "criminals," Equifax said nothing, leaving consumers' data in the hands of "criminals'" unfettered for at least three months between the time the breach started and the time Equifax publically announced it. Incredibly, two days *after* Equifax admitted it detected the breach, company executives sold over $1.8 million of company stock before its collapse on September 8, 2017—when Equifax ultimately did disclose the massive breach. 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 absolutely failed to promptly notify affected consumers once it learned of it.

15. In an exercise of understatement to the extreme, Equifax Chairman and CEO Richard F. Smith stated:[21]

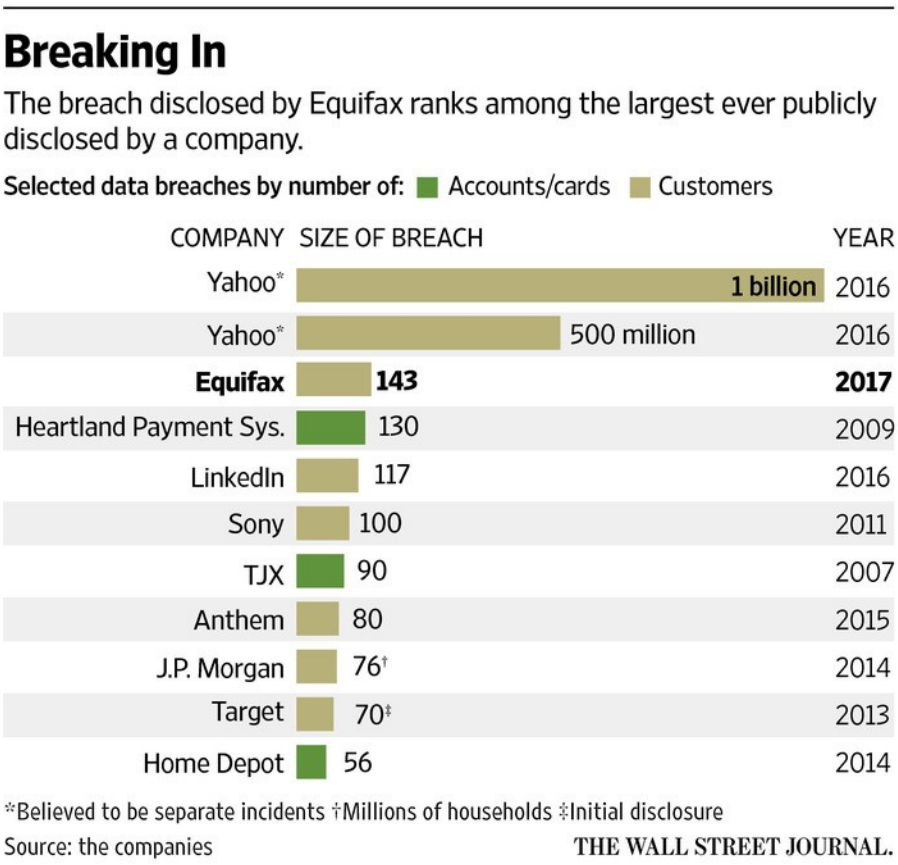
> This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes. **We pride ourselves on being a leader in managing and protecting data**, and we are conducting a thorough review of our overall security operations . . . .

[21] *Id.* (emphasis added).

16. Obviously, Equifax's "pride" in protecting data was misplaced. The massive breach of trust and Equifax's duty to safeguard sensitive data speaks for itself. Equifax did not do nearly enough to protect the consumer data that it stored and used to make its extraordinary profits. All it had to do was install a patch that was publicly known and available to it for months. And there is no possible explanation for its decision to keep this massive data breach secret for six weeks, especially while its own executives dumped stock to avoid the inevitable drop in share price.

17. The Wall Street Journal made the scope of the Equifax breach graphically clear[22]:

[22] *Equifax Reports Data Breach Possibly Affecting 143 Million U.S. Consumers*, Wall Street Journal, Sept. 8, 2017, https://www.wsj.com/articles/equifax-reports-data-breach-possibly-impacting-143-million-u-s-consumers-1504819765 (last accessed Oct. 18, 2017).



18. Alarmingly, and directly evidencing Equifax's woeful and negligent efforts at safeguarding consumers' data, the hack was not particularly sophisticated. As reported by Forbes[23]:

> So how did hackers gain access to the Equifax data? By exploiting a vulnerability on one of the company's U.S.-based web servers. On the surface, at least, that seems to indicate that one of the three major U.S. credit bureaus was victimized by a relatively unsophisticated attack.
>
> Alex Heid, chief security researcher at SecurityScorecard has seen this before. "As surprising as it seems, the same web application vulnerabilities from decades ago are still some of the primary vectors that are leveraged by hackers

[23] *See* https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#34f074f3356f (last access Oct. 16, 2017).

> in modern attack scenarios," he said in a comment to Forbes. Heid added that "it seems that the underlying legacy codebase that handled the [Equifax] web application was vulnerable enough for an attacker to exploit."

19. Equifax knows that it was not doing enough to protect the sensitive information it stored. Chairman and CEO Smith admits: "Confronting cybersecurity risks is a daily fight. While we've made significant investments in data security, ***we recognize we must do more***. And we will."[24] But promises to do better in the future will not help the 143 million U.S. consumers whose complete identities have already been stolen and have, or likely will soon, flood the dark web with everything identity thieves need to destroy consumers' financial lives, wellbeing, and credit.

20. There is little doubt victims of the data breach 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. "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."[25]

---

[24] *See* Equifax Press Release (emphasis added).

[25] *See* Allen St. John, *Equifax Data Breach: What Consumers Need to Know*, CONSUMER REPORTS (updated Sept. 21, 2017), available at https://www.consumerreports.org/privacy/what-consumers-need-to-know-about-the-equifax-data-breach/ (last accessed Oct. 18, 2017).

21. And most affected consumers might never have signed up or agreed to provide their sensitive data to Equifax. Rather, as reported in Yahoo News[26]:

> Unlike a credit card company or retailer, consumers generally don't choose to do business with credit reporting firms. Instead, credit reporting companies gather information on consumers as part of their business.
>
> "The credit bureaus collect highly sensitive consumer data, including Social Security numbers and detailed credit histories, and they have a legal and ethical obligation to protect it," said Jessica Rich, vice president of consumer policy and mobilization at Consumer Reports.
>
> "While it's fine that Equifax is offering consumers free credit card monitoring, that's just a Band-Aid," she added. "Companies need to take data security much more seriously so these breaches don't happen in the first place. That's why we need stronger data security laws with tougher penalties."

22. In addition to selling Equifax consumer data to other fraudsters on the black market, the thieves could use the data to set up fraudulent financial accounts in victims' names, such as credit card accounts.

23. With access to Social Security numbers, birthdates, employment information, and income data, fraudsters could also file false tax returns, with the goal of claiming a fraudulent refund. That's a growing problem in the U.S., with the Internal Revenue Service investigating thousands of false return cases each

---

[26] *See id.*

year.

24. Alarmingly, Equifax has yet to personally notify the particular victims of the data breach, instead setting up a website that renowned security expert Brian Krebs describes as "completely broken at best, and little more than a stalling tactic or sham at worst."[27]

25. Krebs writes[28]:

> WEB SITE WOES
>
> As noted in yesterday's breaking story on this breach, the Web site that Equifax advertised as the place where concerned Americans could go to find out whether they were impacted by this breach — equifaxsecurity2017.com — is completely broken at best, and little more than a stalling tactic or sham at worst.
>
> In the early hours after the breach announcement, the site was being flagged by various browsers as a phishing threat. In some cases, people visiting the site were told they were not affected, only to find they received a different answer when they checked the site with the same information on their mobile phones.
>
> Others (myself included) received not a yes or no answer to the question of whether we were impacted, but instead a message that credit monitoring service we were eligible for was not available and to check back later in the month. The site asked users to enter their last name and last six digits of their SSN, but at the prompting of a

---

[27] *See* Brian Krebs, *Equifax Breach Response Turns Dumpster Fire*, KREBS ON SECURITY (Sept. 8, 2017), available at https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/ (last accessed Oct. 18, 2017).

[28] *See id.*

> reader's comment I confirmed that just entering gibberish names and numbers produced the same result as the one I saw when I entered my real information: Come back on Sept. 13.

26. All the while, the Equifax-described "criminals" have everything they need to open false credit card accounts, bank accounts, loans, and can even file false tax returns and steal refunds owed to consumers whose records have been stolen.

27. Earlier this very year, Equifax's computer security was breached on two separate occasions First, Equifax disclosed that its TALX payroll division was also hacked. As reported by Krebs, "Identity 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 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."[29]

28. Equifax admitted unauthorized access to customers' employee tax records happened between April 17, 2016 and March 29, 2017.[30] For over a year Equifax's customers' employee data was being stolen—and Equifax apparently

---

[29] *See* Brian Krebs, *Fraudsters Exploited Lax Security at Equifax's TALX Payroll Division*, KREBS ON SECURITY (May 18, 2017), available at https://krebsonsecurity.com/2017/05/fraudsters-exploited-lax-security-at-equifaxs-talx-payroll-division/ (last accessed Oct. 18, 2017).

[30] *See id.*

had no idea, or at least did nothing to stop it.

29. Security experts publicly told Equifax that it was not doing enough[31]:

> 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 employment account abuse).

30. 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.[32] 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 the vulnerability

---

31 *See id.*

32 Robert McMillan & AnnaMaria Andriotis, *Equifax Discloses Earlier Cybersecurity Incident, But No Details*, THE WALL STREET JOURNAL (updated Sept. 19, 2017), available at https://www.wsj.com/articles/equifax-discloses-earlier-cybersecurity-incident-but-no-details-1505786212 (last accessed Oct. 16, 2017).

leading to the massive breach which Equifax admits began in May 2017. Equifax re-hired Mandiant in response to the massive, most recent breach.[33]

31. 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 entirely 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.

32. Equifax is currently ranked 703 on the "Fortune 1000" list of top U.S. companies, with $3.145 billion in revenue.[34] Equifax markets and sells consumer information and credit history, including to creditors and prospective creditors who seek such information in the course of selling merchandise, goods, and services. Its profits are uniquely derived from the information it gathers about all consumers, whether or not such consumers have ever purchased anything from Equifax or

---

33 *See id.*

34 http://fortune.com/fortune500/equifax/ (last accessed Oct. 16, 2017).

knowingly provided information to it.

33. 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[35]:

> **Privacy**
>
> For more than 100 years, Equifax has been a catalyst for commerce by bringing businesses and consumers together. Equifax also provides products and services that bring businesses together with other businesses.
>
> 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.

34. There is little question that the above policy demonstrates Equifax was well aware of the need for it to protect consumers' highly valuable personal and financial information, including Personal Identifying Information ("PII"), such as Social Security numbers and driver's license numbers.

35. While Equifax's collection of current customer and associate data may itself be legal, it cannot be questioned that by collecting and storing such extensive and detailed customer data, Equifax creates an obligation for itself to use

[35] *See* Equifax, Privacy, http://www.equifax.com/privacy/ (last accessed Oct. 16, 2017).

every means available to it to protect this data from falling into the hands of criminals. This obligation would obviously include using the latest and strongest methods to prevent website application exploitation, but this is exactly the simplistic attack that led to the massive data breach in this case.

36. In addition to actually securing its data from web application exploitation, by installing publicly available and known critical patches, another rudimentary step Equifax could have and should have taken is encryption. That is, Equifax should have converted consumers' sensitive information into coded strings that would not be immediately useful, or even identifiable 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.

37. As a result of Equifax's unfair, inadequate, and unreasonable data security, cyber-criminals now possess the personal and financial information of Plaintiff and the Proposed Class. 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. With Social Security numbers, names, addresses, birthdates, driver's license numbers, and credit information, criminals can open entirely new credit accounts and bank accounts, and garner millions

through fraud that victims will not be able to detect until it is too late. Victims' credit profiles can be destroyed and they will lose the ability to legitimately borrow money, obtain credit, or even open bank accounts.

38. Further, criminals can file false federal and state tax returns in victim's names, preventing or at least delaying victims' receipt of their legitimate tax refunds and potentially making victims targets of IRS and state tax investigations. At the very least, victims must add themselves to credit fraud watch lists, which substantially impair victims' ability to obtain additional credit. Many experts advise a flat out freeze on all credit accounts, making it impossible to rent a car, get student loans, or buy or rent furniture or a new TV, let alone complete a major purchase such as a new car or home, without taking the time to request that the freeze be suspended, waiting the days it can take for that to occur, and then reinstating the freeze. Further, there are four major reporting agencies, so consumers may need to take these steps with all of them because they will not know which bureau a creditor may consult. Also, in many states, and in many circumstances, such freezes cost the consumer money. Evidently, Equifax will, for a short time, not charge for Equifax freezes—but it is offering no relief for the monetary cost to go through this process at the other three major credit reporting agencies, let alone for the value of time that will be spent doing all of this.

39. Immediate notice of a data breach is essential to obtain the best

protection afforded by identity theft protection services. Equifax failed to provide such immediate notice, thus further exacerbating the damages sustained by Plaintiff and the Proposed Class resulting from the breach. Equifax knew its systems were compromised at least as early as July 29, 2017, yet it made no disclosures until September 7, 2017. Even then, it set up a cryptic website that collected further information, then instructed all consumers, even persons inputting bogus information, to come back later. Such delays are unwarranted, and directly increase the likelihood that thieves will be able to steal victims' identities before victims even know that they are at risk.

40. Personal and financial information is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen credit card numbers, Social Security numbers, and other personal information on a number of Internet websites. A credit card number trades for under $10 on the black market. Magnetic track data increases the price, and a card with full personal information such as an address, phone number, and email address ("fullz") are traded at around $25 per record.[36]

41. But this breach is far more valuable. The data breach consists of over 143 million records that include name, address, birthdate, SSN, drivers' license

[36] Max Cherney, *It's Surprisingly Cheap to Buy Stolen Bank Details*, MOTHERBOARD (Dec. 23, 2013), available at https://motherboard.vice.com/en_us/article/nzewpx/its-surprisingly-cheap-to-buy-stolen-bank-details (last accessed Oct. 16, 2017).

numbers, employment information, and even income. Complete identity records like those at issue here can sell for up to $250 to $400 on the black market, making this a breach potentially worth in excess of $500 billion to cybercriminals.[37]

42. The personal and financial information that Equifax failed to adequately protect, including Plaintiff's identifying information and SSN, are "as good as gold" to identity thieves because identity thieves can use victims' personal data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, and file false federal and state tax returns.

43. Although Equifax is offering free credit monitoring to some customers, the credit monitoring services do little to prevent wholesale identity theft. Moreover, experts warn that batches of stolen information will not be immediately dumped on the black market. In light of the seriousness of this breach and the nature of the data involved, one year of credit monitoring is decidedly not enough.

44. 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

[37] https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report (last accessed Oct. 16, 2017)

thousands of dollars in losses and lost time and productivity. Thus, Plaintiff and the Proposed Class must take additional steps to protect their identities. And Plaintiff and the Proposed Class must bear the burden and expense of identity and credit monitoring, and heightened vigilance for years to come.

PARTIES

45. Defendant Equifax is a Georgia corporation, having its principal place of business in Georgia.

46. Plaintiff Mario Vice is a Louisiana resident. Per the Defendant's advice, Plaintiff used the "Check Potential Impact" and/or "Am I Impacted?" tool at https://www.equifaxsecurity2017.com/am-i-impacted/, which indicated that his personal information may have been compromised. Further, because Equifax has reported that some 143 million U.S. accounts were compromised, it is virtually certain that Plaintiff's data was impacted.

JURISDICTION AND VENUE

47. This Court has diversity jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). Plaintiff and Defendant are citizens of different states. The amount in controversy exceeds $5 million, exclusive of interest and costs, and there are more than 100 putative class members.

48. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Equifax regularly conducts business and resides in this District; a substantial part

of the events, acts, and omissions giving rise to Plaintiff's claims were committed in this District; and property that is the subject of Plaintiff's claims are in this district.

CLASS ALLEGATIONS

49. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action as a class action for himself and all members of the following Proposed Class of similarly situated individuals and entities:

> All residents of the State of Louisiana whose personal and financial information was compromised as a result of the data breach first disclosed by Equifax on or about September 7, 2017.

50. Excluded from the Proposed Class are the Defendant, including any entity in which Defendant has a controlling interest, which is a parent or subsidiary, or which is controlled by the Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendant.

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

52. All members of the Proposed Class are readily ascertainable. Equifax has access to addresses and other contact information for all members of the

Proposed Class, which can be used for providing notice to Proposed Class members.

53. ***Numerosity***. The Proposed Class is so numerous that joinder of all members is unfeasible and not practical. While the precise number of Proposed Class members has not been determined at this time, Equifax has admitted that some 143 million records were breached. Of these millions, the number of Louisiana residents impacted will be sufficiently numerous to merit class certification.

54. ***Commonality***. Questions of law and fact common to all Proposed Class members exist and predominate over any questions affecting only individual Proposed Class members, including, *inter alia*, whether Equifax:

a. Engaged in the wrongful conduct alleged herein;

b. Acted in a manner that was deceptive, unfair, and/or unlawful;

c. Owed a duty to Plaintiff and members of the Proposed Class to adequately protect their personal and financial information;

d. Owed a duty to provide timely and accurate notice of the data breach to Plaintiff and members of the Proposed Class;

e. Used reasonable and industry-standard measures to protect Proposed Class members' personal and financial information;

f. Knew or should have known that its data system was vulnerable to

attack;

g. Acted (or failed to act) in a manner that resulted in (or was the proximate cause of) the breach of its systems, which resulted in the loss of tens of millions of Proposed Class members' personal and financial data;

h. Should have notified the public immediately after it learned of the data breach;

i. Violated state statutory consumer protection, consumer fraud, data-breach-notification, and other applicable laws;

j. Equifax violated state common law as to negligence and otherwise Georgia common law; and

k. Is liable unto Plaintiff and the Proposed Class members for actual damages, statutory damages, and/or punitive damages, restitution, disgorgement, and/or other equitable relief.

55. ***Typicality***. Plaintiff's claims are typical of the claims of the Proposed Class. Plaintiff and all Proposed Class members were injured through the uniform misconduct described above and assert the same claims for relief.

56. ***Adequacy***. Plaintiff and his counsel will fairly and adequately represent the interests of the Proposed Class members. Plaintiff has no interest antagonistic to, or in conflict with, the interests of the Proposed Class members.

Plaintiff's lawyers are highly experienced in the prosecution of consumer class actions and complex commercial litigation.

57. ***Superiority***. A class action is superior to all other available methods for fairly and efficiently adjudicating the claims of Plaintiff and the Proposed Class members. Plaintiff and the proposed Class members have been harmed by Equifax's wrongful actions and/or inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Equifax's wrongful actions and/or inaction.

58. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual members of the Proposed Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

59. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2) because Equifax has acted or refused to act on grounds generally applicable to the Proposed Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Proposed Class as a whole.

60. The expense and burden of litigation would substantially impair the ability of Plaintiff and Proposed Class members to pursue individual lawsuits to vindicate their rights. Absent a class action, Equifax will retain the benefits of its

wrongdoing despite its serious violations of the law.

SUBSTANTIVE GROUNDS FOR RELIEF

COUNT 1 – NEGLIGENCE

61. By accepting and storing Plaintiff's and the Proposed Class members' non-public personal and financial information, including highly sensitive information such as Social Security numbers, driver's license numbers, dates of birth, street addresses, and account information, Equifax assumed a duty, including a special or fiduciary duty, to Plaintiff and the Proposed Class and members requiring it to use reasonable and, at the very least, industry-standard care to secure such information against theft and misuse.

62. Equifax breached its duty of care by failing to adequately secure and protect Plaintiff's and the Proposed Class members' personal and financial information from theft, access, collection, and misuse by third parties.

63. Further, Equifax breached its duty of care by failing to act to protect Plaintiff's and the Proposed Class members' personal and financial information, including, upon information and belief, by neglecting to promptly, completely, and effectively patch and repair its systems when initially advised of one or more critical flaws or vulnerabilities in the Apache Struts Web application framework that it used, or other flaws or vulnerabilities in Apache Struts, or flaws or vulnerabilities in other software, such that the referenced data breach has occurred.

64. Equifax further breached its duty of care by failing to promptly, timely, clearly, accurately, and completely inform Plaintiff's and the Proposed Class that their personal and financial information had been stolen.

65. Plaintiff and members of the Proposed Class have suffered injury in fact, including monetary damages, and will continue to be injured and incur damages as a result of Equifax's negligence and misconduct.

66. As a direct and proximate result of Equifax's failure to take reasonable care and use at least industry-standard measures to protect the personal information placed in its care, Plaintiff and members of the Proposed Class had their personal and financial information stolen, causing direct and measurable monetary losses, threat of future losses, identity theft, and threat of identity theft.

67. As a direct and proximate result of Equifax's negligence and misconduct, Plaintiff and members of the Proposed Class were injured in fact by: identity theft; the loss of the monetary value, including the market value, of their personal and financial information, or PII, due to the data breach, which has led to, or will lead to, its sale on the black market or its presence on dark web sites; 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, all of which have an ascertainable monetary value to be proven at trial.

COUNT 2 – NEGLIGENCE PER SE

68. Plaintiff brings this count on his own behalf and on behalf of the Proposed Class under the laws of the states of Georgia and/or Louisiana.

69. Pursuant to Section 5 of the Federal Trade Commission Act ("FTC Act"), Equifax had a duty to keep and protect the personal information of Plaintiff and Proposed Class members.

70. Equifax violated the FTC Act by failing to keep and protect Plaintiff and Proposed Class members' extremely sensitive and valuable personal and financial information, failing to monitor, and/or failing to ensure that it complied with data security standards, industry standards, statutes, and/or other regulations to protect such personal and financial information. All such omissions were patently unreasonable given the high stakes if malicious actors were to access such information, which they now have done.

71. Equifax violated the FTC Act by failing to safe-keep and protect Plaintiff's and Proposed Class members' personal and financial information, failing to monitor, and/or failing to ensure that Defendant complied with applicable

and current data security standards, statutes, and/or other regulations to protect such personal and financial information.

72. Further, Equifax violated the FTC Act by failing to act to protect Proposed Class members' personal and financial information, including, upon information and belief, by neglecting to promptly patch and repair its systems when advised of one or more critical flaws or vulnerabilities in the Apache Struts Web application framework that it used, or other flaws or vulnerabilities in Apache Struts, or flaws or vulnerabilities in other software, such that the referenced data breach has occurred.

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

74. Plaintiff and members of the Proposed Class have suffered injury in fact, including monetary damages, and will continue to be injured and incur damages as a result of Equifax's negligence *per se*.

75. As a direct and proximate result of Equifax's negligence *per se*, Plaintiff and members of the Proposed Class had their personal and financial information stolen, causing direct and measurable monetary losses, threat of future losses, identity theft, and threat of identity theft.

76. As a direct and proximate result of Equifax's negligence *per se*, Plaintiff and members of the Proposed Class were injured in fact by: identity theft;

the loss of the monetary value, including the market value, of their personal and financial information, or PII, due to the data breach, which has led to, or will lead to, its sale on the black market or its presence on dark web sites; 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, all of which have an ascertainable monetary value to be proven at trial.

COUNT 3 – VIOLATION OF THE GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT

77. Plaintiff, the Proposed Class, and Equifax are "persons" within the meaning of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA"), Ga. Code § 10- 1-371(5).

78. The Georgia UDTPA prohibits "deceptive trade practices," which include the "misrepresentation of standard or quality of goods or services," and "engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding." Ga. Code § 10-1-372(a).

79. In the course of its business, Equifax willfully failed to disclose and

actively concealed its grave data-security defects as discussed herein, and otherwise engaged in activities with a tendency or capacity to deceive. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of material facts with intent that others rely upon such concealment, suppression, or omission, in connection with accessing and storing the extremely sensitive and valuable personal and financial information of Plaintiff and Proposed Class members. Equifax did all of this directly with respect to Plaintiff and Proposed Class members, and also by way of their transactions as to goods, merchandise, and services with prospective creditors and creditors who also accessed their extremely sensitive and valuable personal and financial in the course of those transactions.

80. For months, Equifax knew of vulnerabilities and defects in its data-security systems, and vulnerabilities in key databases storing the extremely sensitive and valuable personal and financial information of Plaintiff and Proposed Class members, but concealed all of that information.

81. Equifax was also aware that it valued profits over real and effective data security. Equifax concealed this information as well.

82. By way of the foregoing, Equifax engaged in deceptive business practices in violation of the Georgia UDTPA. Equifax also engaged in deceptive

acts and practices in at least the following ways:

a. Equifax misrepresented material facts (intending for others to rely upon the misrepresentations) to the Proposed Class by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Proposed Class members' personal and financial information from unauthorized disclosure, release, data breaches, and theft;

b. Equifax misrepresented material facts (intending for others to rely upon the misrepresentations) to the Proposed Class by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Proposed Class members' personal and financial information;

c. Equifax omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for Proposed Class members' personal and financial information, with the intent that others rely on the omission, suppression, and concealment;

d. Equifax engaged in deceptive acts and practices by failing to maintain the privacy and security of Proposed Class members' personal and financial information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the

data breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45), the Gramm-Leach-Bliley Act (15 U.S.C. § 6801) and its Safeguards Rule, as well as the Georgia Code (O.C.G.A.) § 10-1-911, *et seq.*;

e. Equifax engaged in deceptive acts and practices by failing to disclose the data breach to Proposed Class members in a timely and accurate manner, in violation of Ga. Code § 10-1-912;

f. Equifax engaged in deceptive acts and practices by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Proposed Class members' personal and financial information from further unauthorized disclosure, release, data breaches, and theft.

83. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including the Plaintiff and Proposed Class members, regarding the security and safety of its databases and the extremely sensitive and valuable personal and financial information of the Plaintiff and Proposed Class members.

84. Equifax intentionally and knowingly misrepresented such material facts with an intent to mislead Plaintiff and Proposed Class members.

85. Equifax knew or should have known that its conduct violated the Georgia UDTPA. As alleged above, Equifax made material statements that were either false or misleading.

86. Equifax owed the Plaintiff and Proposed Class a duty to disclose the true facts regarding data-security defects and vulnerabilities because Equifax:

a. Possessed exclusive knowledge that it valued profits and cost-cutting over the safety of the extremely sensitive and valuable personal and financial information of Plaintiff and Proposed Class members;

b. Intentionally concealed the foregoing from Plaintiff and the Proposed Class; and/or

c. Made incomplete representations regarding these matters while purposefully withholding material facts from Plaintiff and the Proposed Class that contradicted these representations.

87. Equifax's representations and omissions were material to the Plaintiff and Proposed Class given the extreme sensitivity and value of their personal and financial information.

88. Plaintiff and the Proposed Class suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information as alleged herein.

89. Equifax had an ongoing duty to all Equifax customers, including

Plaintiff and the Proposed Class members, to refrain from unfair and deceptive practices under the Georgia UDTPA.

90. Equifax's violations present a continuing risk to the Plaintiff and Proposed Class members, as well as to the general public. Equifax's unlawful acts and practices complained of herein affect the public interest.

91. As a direct and proximate result of Equifax's violations of the Georgia UDTPA, Plaintiff and Proposed Class members have suffered injury-in-fact and/or actual damage. Plaintiff seeks an order enjoining Equifax's unfair, unlawful, and/or deceptive practices, attorneys' fees, and any other just and proper relief available under the Georgia UDTPA per Ga. Code § 10-1-373.

COUNT 4 – VIOLATION OF THE LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, LA. REV. STAT. §§ 51:1401, *ET SEQ.*

92. Equifax, Plaintiff, and the Proposed Class members are "persons" within the meaning of the La. Rev. Stat. § 51:1402(8).

93. Plaintiff and the Proposed Class members are "consumers" within the meaning of La. Rev. Stat. § 51:1402(1).

94. Equifax engaged in "trade" or "commerce" within the meaning of La. Rev. Stat. § 51:1402(10).

95. The Louisiana Unfair Trade Practices and Consumer Protection Law ("Louisiana CPL") makes unlawful "deceptive acts or practices in the conduct of

any trade or commerce." La. Rev. Stat. § 51:1405(A). Equifax participated in misleading, false, or deceptive acts that violated the Louisiana CPL.

96. In the course of its business, Equifax willfully failed to disclose and actively concealed the facts discussed herein and otherwise engaged in activities with a tendency or capacity to deceive. Equifax also engaged in unlawful trade practices by employing deception, deceptive acts or practices, fraud, misrepresentations, or concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression, or omission, in connection with its use and storage of consumers personal and financial information.

97. Equifax knew it had not taken adequate steps to protect consumer's personal and financial information from theft, as represented. Equifax knew this for at least several months, but concealed all of that information.

98. Equifax was also aware that it valued profits over the security of consumers' personal and financial information, and that its data systems were not secure and that it had suffered multiple data breaches. Equifax concealed this information as well.

99. By failing to disclose that its computer and data systems were not secure, and by presenting itself as a reputable company that valued data security, Equifax engaged in deceptive business practices in violation of the Louisiana CPL.

100. Equifax's unfair or deceptive acts or practices were likely to and did in fact deceive reasonable consumers, including Plaintiff and the other Proposed Class members, about the true security of its computer and data systems and the devaluing data security at Equifax.

101. Equifax intentionally and knowingly misrepresented material facts regarding the security of consumers' personal and financial information with an intent to mislead Plaintiff and the Proposed Class.

102. Equifax knew or should have known that its conduct violated the Louisiana CPL. As alleged above, Equifax made material statements about the safety and security of personal and financial information that were either false or misleading.

103. Equifax owed the Proposed Class a duty to disclose the true lack of security of its computer and data systems because Equifax:

a. Possessed exclusive knowledge that it valued profits over data security;

b. Intentionally concealed the foregoing from the Plaintiff and the Proposed Class; and/or

c. Made incomplete representations about the security of its computer and data systems generally, and that it had suffered data breaches in particular, while purposefully withholding material facts from

Plaintiff and the Proposed Class that contradicted these representations.

104. Equifax's fraudulent representations were material to Plaintiff and the Proposed Class.

105. Plaintiff and the Proposed Class have suffered ascertainable loss caused by Equifax's misrepresentations and its concealment of and failure to disclose material information as alleged herein, including time and expenses associated with securing their identities from theft, including costs to implement and maintain credit freezes and identity theft monitoring and protection.

106. Equifax had an ongoing duty to all Proposed Class members to refrain from unfair and deceptive practices under the Louisiana CPL. All members suffered ascertainable loss in the form of out-of-pocket costs and loss of time as a result of Equifax's deceptive and unfair acts and practices made in the course of Equifax's business.

107. Equifax's violations present a continuing risk to the Proposed Class. Equifax's unlawful acts and practices complained of herein affect the public interest.

108. As a direct and proximate result of Equifax's violations of the Louisiana CPL, Plaintiff and the Proposed Class have suffered injury-in-fact and/or actual damage.

109. Pursuant to La. Rev. Stat. § 51:1409, Plaintiff and the Proposed Class seek to recover actual damages in an amount to be determined at trial; treble damages for Equifax's knowing violations of the Louisiana CPL; an order enjoining Equifax's unfair, unlawful, and/or deceptive practices; declaratory relief; attorneys' fees; and any other just and proper relief available under La. Rev. Stat. § 51:1409.

COUNT 5 – VIOLATION OF THE LOUISIANA DATA BREACH STATUTE, LA. REV. STAT. § 3074, *ET SEQ.*

110. Equifax is required to accurately notify Plaintiff and Proposed Class members if it becomes aware of a breach of its data security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and the Proposed Class members' personal and financial information) in the most expedient time possible and without unreasonable delay under La. Rev. Stat. § 51:3074(C).

111. Defendant is a business that owns or licenses computerized data that includes personal information as defined by La. Rev. Stat. § 51:3074(C).

112. Plaintiff's and the Proposed Class members' personal and financial information (*e.g.*, Social Security numbers) includes personal information as covered under La. Rev. Stat. § 51:3074(C).

113. Because Equifax was aware of a breach of its security system (was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and the

Proposed Class members' personal and financial information), Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by La. Rev. Stat. § 51:3074(C).

114. As a direct and proximate result of Equifax' violations of La. Rev. Stat. § 51:3074(C), Plaintiff and the Proposed Class members suffered damages, as described above.

115. Plaintiff and the Proposed Class members seek relief under La. Rev. Stat. § 51:3075, including, but not limited to, actual damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the following relief:

a. The proposed Class be certified, and that the named Plaintiff be named as Class Representative, and his counsel be appointed as Class Counsel;

b. Plaintiff and the Proposed Class be awarded appropriate relief, including actual and statutory damages, disgorgement, and restitution, and punitive, including under O.C.G.A. § 51-12-5.1, exemplary, or multiple damages where available;

c. Plaintiff and the Proposed Class be awarded preliminary or other equitable or declaratory relief as may be appropriate by way of applicable state or federal law;

d. Such additional orders or judgments as may be necessary to prevent these

practices and to restore to any person in interest any money or property which may have been acquired by means of the violations; and

e. Plaintiff and the Proposed Class be awarded such other, favorable relief as may be available and appropriate under law or at equity.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all issues so triable.

Respectfully submitted, this 25th day of October, 2017.

ROBBINS GELLER RUDMAN & DOWD LLP

By */s/ John C. Herman*
JOHN C. HERMAN
(Ga. Bar No. 348370)
CARLTON R. JONES
(Ga. Bar No. 940540)
3424 Peachtree Road, N.E., Suite 1650
Atlanta, GA 30326
Telephone: 404/504-6500
Facsimile: 404/504-6501
jherman@rgrdlaw.com
cjones@rgrdlaw.com

ROBBINS GELLER RUDMAN & DOWD LLP
PAUL J. GELLER (*pro hac vice* to be filed)
STUART A. DAVIDSON (*pro hac vice* to be filed)
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Telephone: 561/750-3000
Facsimile: 561/750-3364
pgeller@rgrdlaw.com
sdavidson@rgrdlaw.com

BURNS CHAREST LLP
KOREY A. NELSON (*pro hac vice* to be filed)
C. JACOB GOWER (*pro hac vice* to be filed)
365 Canal Street, Suite 1170
New Orleans, LA 70139
Telephone: 504/799-2845
Facsimile: 504/881-1765
knelson@burnscharest.com
jgower@burnscharest.com

BURNS CHAREST LLP
WARREN T. BURNS (*pro hac vice* to be filed)
DANIEL H. CHAREST (*pro hac vice* to be filed)
900 Jackson Street, Suite 500
Dallas, Texas 75202
Telephone: 469/904-4550
Facsimile: 469/444-5002
wburns@burnscharest.com
dcharest@burnscharest.com

Attorneys for Plaintiff and the Proposed Classes

JS44 (Rev. 6/2017 NDGA)

CIVIL COVER SHEET

The JS44 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 is required for the use of the Clerk of Court for the purpose of initiating the civil docket record. (SEE INSTRUCTIONS ATTACHED)

I. (a) PLAINTIFF(S)

MARIO VICE, Individually and on Behalf of All Others Similarly Situated

DEFENDANT(S)

EQUIFAX INC., a Delaware corporation

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF Louisiana
(EXCEPT IN U.S. PLAINTIFF CASES)

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

(c) ATTORNEYS (FIRM NAME, ADDRESS, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

JOHN C. HERMAN
ROBBINS GELLER RUDMAN & DOWD LLP
3424 Peachtree Road, N.E., Suite 1650
Atlanta, GA 30326
(404) 504-6500, jherman@rgrdlaw.com

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)

PLF	DEF		PLF	DEF	
☐ 1	☐ 1	CITIZEN OF THIS STATE	☐ 4	☑ 4	INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE
☑ 2	☐ 2	CITIZEN OF ANOTHER STATE	☐ 5	☐ 5	INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE
☐ 3	☐ 3	CITIZEN OR SUBJECT OF A FOREIGN COUNTRY	☐ 6	☐ 6	FOREIGN NATION

IV. 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 District)
- ☐ 6 MULTIDISTRICT LITIGATION - TRANSFER
- ☐ 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT
- ☐ 8 MULTIDISTRICT LITIGATION - DIRECT FILE

V. 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)

Class Action Fairness Act, 28 U.S.C. § 1332(d)(2).

(IF COMPLEX, CHECK REASON BELOW)

- ☐ 1. Unusually large number of parties.
- ☐ 2. Unusually large number of claims or defenses.
- ☐ 3. Factual issues are exceptionally complex
- ☐ 4. Greater than normal volume of evidence.
- ☐ 5. Extended discovery period is needed.
- ☐ 6. Problems locating or preserving evidence
- ☐ 7. Pending parallel investigations or actions by government.
- ☐ 8. Multiple use of experts.
- ☐ 9. Need for discovery outside United States boundaries.
- ☐ 10. Existence of highly technical issues and proof.

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT $_____ APPLYING IFP _____ MAG. JUDGE (IFP) _____

JUDGE _____ MAG. JUDGE _____ NATURE OF SUIT _____ CAUSE OF ACTION _____
(Referral)

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)

CONTRACT - "0" MONTHS DISCOVERY TRACK
- ☐ 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- ☐ 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- ☐ 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK
- ☐ 110 INSURANCE
- ☐ 120 MARINE
- ☐ 130 MILLER ACT
- ☐ 140 NEGOTIABLE INSTRUMENT
- ☐ 151 MEDICARE ACT
- ☐ 160 STOCKHOLDERS' SUITS
- ☐ 190 OTHER CONTRACT
- ☐ 195 CONTRACT PRODUCT LIABILITY
- ☐ 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 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 - "4" MONTHS DISCOVERY TRACK
- ☐ 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
- ☐ 365 PERSONAL INJURY - PRODUCT LIABILITY
- ☐ 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- ☐ 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☑ 370 OTHER FRAUD
- ☐ 371 TRUTH IN LENDING
- ☐ 380 OTHER PERSONAL PROPERTY DAMAGE
- ☐ 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK
- ☐ 422 APPEAL 28 USC 158
- ☐ 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 440 OTHER CIVIL RIGHTS
- ☐ 441 VOTING
- ☐ 442 EMPLOYMENT
- ☐ 443 HOUSING/ ACCOMMODATIONS
- ☐ 445 AMERICANS with DISABILITIES - Employment
- ☐ 446 AMERICANS with DISABILITIES - Other
- ☐ 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK
- ☐ 462 NATURALIZATION APPLICATION
- ☐ 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK
- ☐ 463 HABEAS CORPUS- Alien Detainee
- ☐ 510 MOTIONS TO VACATE SENTENCE
- ☐ 530 HABEAS CORPUS
- ☐ 535 HABEAS CORPUS DEATH PENALTY
- ☐ 540 MANDAMUS & OTHER
- ☐ 550 CIVIL RIGHTS - Filed Pro se
- ☐ 555 PRISON CONDITION(S) - Filed Pro se
- ☐ 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK
- ☐ 550 CIVIL RIGHTS - Filed by Counsel
- ☐ 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK
- ☐ 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- ☐ 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK
- ☐ 710 FAIR LABOR STANDARDS ACT
- ☐ 720 LABOR/MGMT. RELATIONS
- ☐ 740 RAILWAY LABOR ACT
- ☐ 751 FAMILY and MEDICAL LEAVE ACT
- ☐ 790 OTHER LABOR LITIGATION
- ☐ 791 EMPL. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 820 COPYRIGHTS
- ☐ 840 TRADEMARK

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK
- ☐ 830 PATENT
- ☐ 835 PATENT-ABBREVIATED NEW DRUG APPLICATIONS (ANDA) - a/k/a Hatch-Waxman cases

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK
- ☐ 861 HIA (1395ff)
- ☐ 862 BLACK LUNG (923)
- ☐ 863 DIWC (405(g))
- ☐ 863 DIWW (405(g))
- ☐ 864 SSID TITLE XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK
- ☐ 870 TAXES (U.S. Plaintiff or Defendant)
- ☐ 871 IRS - THIRD PARTY 26 USC 7609

OTHER STATUTES - "4" MONTHS DISCOVERY TRACK
- ☐ 375 FALSE CLAIMS ACT
- ☐ 376 Qui Tam 31 USC 3729(a)
- ☐ 400 STATE REAPPORTIONMENT
- ☐ 430 BANKS AND BANKING
- ☐ 450 COMMERCE/ICC RATES/ETC.
- ☐ 460 DEPORTATION
- ☐ 470 RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS
- ☐ 480 CONSUMER CREDIT
- ☐ 490 CABLE/SATELLITE TV
- ☐ 890 OTHER STATUTORY ACTIONS
- ☐ 891 AGRICULTURAL ACTS
- ☐ 893 ENVIRONMENTAL MATTERS
- ☐ 895 FREEDOM OF INFORMATION ACT
- ☐ 899 ADMINISTRATIVE PROCEDURES ACT / REVIEW OR APPEAL OF AGENCY DECISION
- ☐ 950 CONSTITUTIONALITY OF STATE STATUTES

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK
- ☐ 410 ANTITRUST
- ☐ 850 SECURITIES / COMMODITIES / EXCHANGE

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK
- ☐ 896 ARBITRATION (Confirm / Vacate / Order / Modify)

*** PLEASE NOTE DISCOVERY TRACK FOR EACH CASE TYPE. SEE LOCAL RULE 26.3**

VII. REQUESTED IN COMPLAINT:

☑ **CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23** **DEMAND $** 5,000,000+

JURY DEMAND ☑ **YES** ☐ **NO (CHECK YES ONLY IF DEMANDED IN COMPLAINT)**

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE Not Assigned **DOCKET NO.** MDL No. 2800

CIVIL CASES ARE DEEMED RELATED IF THE PENDING CASE INVOLVES: (CHECK APPROPRIATE BOX)

- ☐ **1. PROPERTY INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☑ **2. SAME ISSUE OF FACT OR ARISES OUT OF THE SAME EVENT OR TRANSACTION INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **3. VALIDITY OR INFRINGEMENT OF THE SAME PATENT, COPYRIGHT OR TRADEMARK INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.**
- ☐ **4. APPEALS ARISING OUT OF THE SAME BANKRUPTCY CASE AND ANY CASE RELATED THERETO WHICH HAVE BEEN DECIDED BY THE SAME BANKRUPTCY JUDGE.**
- ☐ **5. REPETITIVE CASES FILED BY PRO SE LITIGANTS.**
- ☐ **6. COMPANION OR RELATED CASE TO CASE(S) BEING SIMULTANEOUSLY FILED (INCLUDE ABBREVIATED STYLE OF OTHER CASE(S)):**

☐ **7. EITHER SAME OR ALL OF THE PARTIES AND ISSUES IN THIS CASE WERE PREVIOUSLY INVOLVED IN CASE NO. , WHICH WAS DISMISSED. This case ☐ IS ☐ IS NOT (check one box) SUBSTANTIALLY THE SAME CASE.**

/s/ John C. Herman — October 25, 2017

SIGNATURE OF ATTORNEY OF RECORD **DATE**

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

UNITED STATES DISTRICT COURT

for the

Northern District of Georgia

MARIO VICE, Individually and on Behalf of All Others Similarly Situated

Plaintiff(s)

v.

EQUIFAX INC., a Delaware corporation

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.
Atlanta, GA 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: JOHN C. HERMAN
ROBBINS GELLER RUDMAN & DOWD LLP
Monarch Centre, Suite 1650
3424 Peachtree Road, N.E.
Atlanta, GA 30326
Telephone: (404) 504-6500

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: