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

CASE NO:

BARBARA J. DOMINO, DANIEL E. ALMEIDA, and MIRIAM CEJAS,
Florida consumers individually and on behalf of all others similarly situated,

Plaintiffs,

v.

EQUIFAX, INC.

Defendant.

CLASS ACTION COMPLAINT

Negligence

28 U.S.C. § 1332

DEMAND FOR JURY TRIAL

Plaintiffs BARBARA J. DOMINO ("DOMINO"), DANIEL E. ALMEIDA ("ALMEIDA"), and MIRIAM CEJAS ("CEJAS") (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, by and through their undersigned attorneys, hereby bring this Class Action Complaint against EQUIFAX, INC. ("Equifax") ("Defendant"), and allege as follows:

1) The allegations in this Class Action Complaint are based on the personal knowledge of each of the Plaintiffs as to themselves and on information and belief as to all other matters, through investigation of Plaintiffs' undersigned counsel. Plaintiffs believe substantial evidentiary support exists for the allegations set forth herein after a reasonable opportunity for discovery.

SUMMARY OF THE CASE

2) Plaintiffs allege, on behalf of themselves and all others similarly situated (the "Class" or "Classes" as defined below) that from mid-May through July 2017 criminals exploited an

Equifax data server, gaining access to their internal database storage systems and millions of consumer data records. According to an announcement by defendant Equifax, *"most of the consumer information accessed 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 consumers and certain dispute documents, which included personal identifying information, for approximately 182,000 consumers, were accessed."* (from Equifax Cybersecurity Incident – Information & Support webpage, paragraphs I - II, September 14, 2017).

3) Even though defendant Equifax discovered the unauthorized data breach on July 29, 2017, the company intentionally withheld disclosing the data breach to the public, jeopardizing consumer's personal and financial information and subjecting them to possible financial losses now or in the future. Defendant Equifax finally disclosed the data breach some six weeks later, on September 7, 2017.

4) Defendant Equifax's response to the data breach was haphazard and slow. During that six-week period, defendant Equifax negligently allowed U.S. consumers to be exposed to identity theft, fraud and financial loss by failing to exercise reasonable security precautions, failing to comply with industry standards for processing, storing and/or allowing access to consumer personal, financial and credit information. Had defendant Equifax taken the necessary precautions to protect its data, it would have prevented the breach altogether or at least detected the breach much earlier, reducing the harm U.S. consumers are now facing.

5) Defendant Equifax is well aware that securing the personal information it gathers is central to its business. Equifax CEO and Chairman Richard Smith acknowledged as much in his statement about the breach: *"This is entirely 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."*

6) Due to defendant Equifax's negligence and failure to protect its data, failure to notice the Florida Department of Legal Affairs as required by law, issue and warn consumers as soon as it learned of the data breach in a timely fashion, Defendant Equifax, by its negligence and subsequent inaction, allowed consumers to be victimized without their knowledge and were therefore left without the ability to take any countermeasures to prevent fraud, identity theft, financial loss and/or damage to their credit history and credit scores.

7) As further proof of defendant Equifax's negligence and possible reason for withholding public disclosure, three of Equifax's top executives sold over $1.8 million in company stock after discovery of the data breach but before its public disclosure, a sale that was not part of any option-exercise program. The sales were made on August 1 and 2, 2017, the third and fourth days after the breach was discovered by:

a. John Gamble, Chief Financial Officer and Corporate Vice President of the company and one of the persons who would normally be notified immediately of any such data breach (because any such breach would have a negative impact on the finances of the company and devalue the stock price). Mr. Gamble sold 6,500 shares at $145.60, netting approximately $946,374. Following the company's disclosure of the data breach, its share prices dropped and were recently trading at $123, which means that if Mr. Gamble had waited to sell after the breach was disclosed, it would have cost him over $140,000.

b. Joseph Loughran, President of U.S. Information Solutions, sold $584,099 in shares;

c. and Rodolfo Ploder, President of Workforce Solutions, sold $250,458 in shares.

8) In an egregious attempt to profit from this catastrophic data breach, defendant Equifax created a website for consumers to allow them to check to see if their information was compromised, and regardless of the search result, users are invited to sign up for defendant Equifax's "TrustedID Premier" credit monitoring service, and as a recompense to the data breach victims, defendant Equifax is offering the service free for one year, after which consumers would have to pay $19.95 per month. In fact, enrollment in defendant Equifax's "TrustedID Premier" service requires that consumers again provide

defendant with their full name, social security number and other personal, sensitive information, in addition to a valid credit card number, which the company will use to automatically bill consumers after their free one-year enrollment expires.

9) Additionally and deceptively, defendant Equifax does not make it clear to consumers that enroll in defendant Equifax's "TrustedID Premier" service that when they enroll in the service the consumer surrendering their right to sue defendant Equifax, effectively preventing the consumer from filing or joining any class action against the defendant. Instead, the consumer would he forced into arbitration with no redress in a court of law.

10) Plaintiffs Barbara J. Domino, Daniel E. Almeida and Mirian Cejas are consumers who bring this proposed class action lawsuit on behalf of Florida consumers alleging that defendant Equifax failed to adequately safeguard consumer's personal, credit and identity information in compliance with applicable rules, statutes and industry standards.

11) Plaintiffs seek injunctive relief requiring defendant Equifax to invest in security, security monitoring, and comply with data security standards and regulations designed to prevent these types of breaches, damages, restitution and other remedies.

THE PARTIES

12) Equifax Inc. ("Equifax") is a global, multi-billion dollar Atlanta, Georgia corporation with interests and investments in 24 countries, with operating revenues of $3,144,900,000 in fiscal year 2016, that provides credit information services to millions of businesses, governmental units, and consumers across the globe. Equifax operates through various subsidiaries including Equifax Information Services, LLC, and Equifax Consumer Services, LLC aka Equifax Personal Solutions a/k/a "PSOL". Each of these entities acted as agents of Equifax or in the alternative, acted in concert with Equifax as alleged in this complaint.

13) Barbara J. Domino ("DOMINO") is an individual consumer residing in Miramar, Florida, whose name was included in the list of records stolen and who was affected by the data breach announced by Defendant Equifax in September 2017.

14) Miriam Cejas ("CEJAS") is an individual consumer residing in Miramar, Florida, whose name was included in the list of records stolen and who was affected by the data breach announced by Defendant Equifax in September 2017.

15) Daniel E. Almeida ("ALMEIDA") is an individual consumer residing in Cooper City, Florida, whose name was included in the list of records stolen and who was affected by the data breach announced by Defendant Equifax in September 2017.

JURISDICTION AND VENUE

16) This Court has original jurisdiction pursuant to the Class Action Fairness Act, under 28 U.S.C. § 1332(d), because

(a) at least one member of the putative class is a citizen of Florida, a different state from defendant Equifax, whose principal place of business is Atlanta, Georgia:

(b) the amount in controversy exceeds $5,000,000, exclusive of penalties, interest and costs;

(c) the proposed class action consists of more than 100 class members, and

(d) none of the exceptions under the subsection apply to this action.

17) This Court has jurisdiction over defendant Equifax because Equifax, Inc., is registered to conduct business in Florida, has sufficient contacts in Florida or otherwise intentionally avails itself of the markets within Florida, through the promotion, sale, marketing and/or distribution of its products and services in Florida, to render the exercise of jurisdiction by this Court proper and necessary.

18) Venue is proper in this District under 28 U.S.C. § 1391 because Plaintiffs reside in this district and a substantial part of the events giving rise to Plaintiff's claims occurred in this district.

FACTUAL ALLEGATIONS

19) Plaintiffs file this complaint as a national class action on behalf of over 143 million consumers (approximately 43% of all Americans) across the country harmed by Defendant Equifax's failure to adequately protect their private credit and personal information. We estimate that approximately 8 million Floridians have been affected. This complaint requests defendant Equifax provide fair compensation in an amount that will ensure every consumer harmed by its data breach will not be out-of-pocket for the costs of independent third-party credit repair and monitoring services. This complaint's allegations are based on personal knowledge as to plaintiffs' conduct and made on information and belief as to the acts of others.

20) Throughout the past year, without the consent of the Plaintiffs, Equifax collected and stored personal and credit information from Plaintiffs Ms. Domino, Mr. Almeida and Ms. Cejas including their full name, social security numbers, birth dates, home addresses, driver's license information, income, employment, employment history, credit card numbers and other private and personal information.

21) Equifax owed a legal duty to consumers like Ms. Domino, Mr. Almeida and Ms. Cejas to use reasonable care to protect their credit and personal information from unauthorized access by third parties. Equifax knew that its failure to protect Plaintiff's personal and credit information from unauthorized access would cause serious risks of credit harm, financial loss and identify theft for years to come.

22) On September 7, 2017, Equifax announced for the first time that from May to July 2017, its database storing Ms. Domino, Mr. Almeida and Ms. Cejas' credit and personal information, and that of millions of other Americans, had been hacked by unauthorized

third parties, subjecting Ms. Domino, Mr. Almeida and Ms. Cejas and all others contained in the list of records stolen to credit harm, financial loss and identify theft.

23) In an attempt to increase profits, Equifax negligently failed to maintain adequate technological safeguards to protect Ms. Domino, Mr. Almeida and Ms. Cejas' information from unauthorized access by hackers. Equifax knew and should have known that failure to maintain adequate technological safeguards would eventually result in a massive data breach and loss. Equifax could have and should have substantially increased the amount of money it spent to protect against cyber-attacks but chose not to. Consumers like Ms. Domino, Mr. Almeida and Ms. Cejas should not have to bear the expense caused by Equifax's negligent failure to safeguard their credit and personal information from cyber-attackers.

24) Equifax is one of the three major credit reporting agencies in the United States. As a credit reporting agency, Equifax is engaged in a number of credit-related services and holds itself out as "*a consumer advocate, steward of financial literacy, and champion of economic advancement" and "an innovative global information solutions company that enables access to credit.*" (http://www.equifax.com/about-equifax/)

25) Prior to the Data Breach, Equifax promised its customers and everyone else whose Personal Information it collects that it would reasonably protect their Personal Information. Equifax's privacy policy stated, in relevant part, that: "*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***." (http://www.equifax.com/privacy/).

26) Equifax maintains multiple "privacy policies" that purport to apply to different sects of its customers or consumers. For example, Equifax's privacy policy related to "Activities by Consumers Related to Credit Reports" states that:

> **Information Collection and Use**
> We collect personal and non-personal information on our web site to fulfill your requests and contact you. There are aspects of our site that can be enjoyed as a visitor, but you need to provide us with personal information in order to perform Consumer Activities associated with your credit file, such as requesting an annual disclosure of your credit file, disputing of information in your credit file, or placing a security freeze or an initial fraud alert.
>
> **Information We Collect From You**
> **Contacting Equifax with a request:** We receive information from you when you perform one of the Consumer Activities through our site. We also receive information from you when you register for an Equifax Personal Solutions account in order to maintain online access to your free annual credit file disclosure for 30 days. This information may include:
> • First and last name (middle initial and suffix, as applicable);
> • Social Security number;
> • Date of birth;
> • Home telephone number;
> • E-mail address;
> • Current and former mailing address; and
> • Credit card number and expiration date.
>
> **Log information:** When you visit our site, our servers automatically collect log information. This information may include your web page request, Internet Protocol (IP) address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your browser. We collect log information so that we can properly administer our system and gather aggregate information about how our site is being used, including the pages visitors are viewing on our site.

Information We Collect From Others

We also collect information about you from third parties, including AnnualCreditReport.com (the centralized service for consumers to request their free annual credit reports), parties from whom we request information in connection with your request for dispute resolution, the centralized pre-screening opt-out management service, and other credit reporting agencies when you place initial fraud or active duty alerts.

When we associate information that we obtain from third parties with personal information that we have collected under this policy, we will treat the acquired information like the information that we collected ourselves. We will not share information we obtain from third parties in personally identifiable form. However, we may share aggregated, non-personal information as described in this policy, including information we obtained from third parties, in a form that will not allow you to be identified.

How We Use Collected Information

We use the information we collect about you to administer our web site, improve the user experience, and provide you with the information or services you request. In connection with your one or more Consumer Activities, we will use your email address to communicate with you regarding the status of your online request.

To Whom We May Disclose the Information We Collect

We take reasonable precautions to be sure that nonaffiliated third parties and affiliates to whom we disclose your personally identifiable information are aware of our privacy policy and will treat the information in a similarly responsible manner. Our contracts and written agreements with nonaffiliated third parties that receive information from us about you prevent further transfer of the information. We will ***not disclose*** your personal information to third parties except to provide you with the disclosure or service you request, or under certain circumstances as described in this policy (http://www.equifax.com/privacy/personal-credit-reports).

27) By permitting unauthorized access to consumers' Personal Information, Equifax failed to comply with its own privacy policy.

28) There is no question Equifax recognizes the risks of a data breach because it markets and sells "data breach solutions" to consumers and businesses. In its marketing materials, Equifax states: "*You'll feel safer with Equifax. We're the leading provider of data breach services, serving more than 500 organizations with security breach events everyday. In addition to extensive experience, Equifax has the most comprehensive set of identity theft products and customer service coverage in the market.*" (http://www.equifax.com/help/data-breach-solutions/).

29) Equifax has a history of major data security problems. In 2010, tax forms mailed by Equifax's payroll vendor had Equifax employees' SSNs partially or fully viewable through the envelope's return address window. One affected Equifax employee stated "If they can't do this internally how are they going to be able to go to American Express and other companies and say we can mitigate your liability? They are first-hand delivering information for the fraudsters out there. It's so terribly sad. It's just unacceptable, especially from a credit bureau." (Elinor Mills, *Equifax Tax Forms Expose Worker Social Security Numbers*, CNET, (Feb. 11, 2010), http://www.cnet.com/news/equifax-tax-forms-expose-worker-social-securitynumbers/ (September 10, 2017).

30) In March 2013, Equifax confirmed "fraudulent and unauthorized" access to the credit reports of multiple celebrities and top Washington, D.C. officials, including First Lady Michelle Obama and Vice President Joe Biden. (*U.S. Probes Hack of Credit Data on Mrs. Obama, Beyonce, Others*, REUTERS, (March 12, 2013), http://www.reuters.com/article/us-usa-cybersecurity-hacking-idUSBRE92B12520130313 (September 10, 2017).

31) In March 2015, Equifax notified certain consumers that personal information contained on their credit file was erroneously sent to unauthorized individuals due to a technical error during a software change. (*Data Incident Notification to New Hampshire Attorney*

General, (April 2, 2015), http://doj.nh.gov/consumer/security-breaches/documents/equifax-20150402.pdf (September 10, 2017).

32) Also in March 2015, Equifax mistakenly sent a Maine woman the full credit reports of more than 300 other individuals, which exposed their SSNs, dates of birth, current and previous addresses, creditor information, and bank and loan account numbers, among other sensitive information. The woman told reporters *"I'm not supposed to have this information, this is unbelievable, someone has messed up."* (Jon Chrisos, *Credit Agency Mistakenly Sends 300 Confidential Reports to Maine Woman*, BANGOR DAILY NEWS, (March 19, 2015), http://bangordailynews.com/2015/03/19/news/state/credit-agency-mistakenly-sends-300-confidential-reports-to-maine-woman/ (September 10, 2017)

33) In May 2016, it was discovered that a product offered by Equifax's subsidiary company Equifax Workforce Solutions, Inc. (d/b/a TALX), a purveyor of products and services related to Human Resources, payroll, and tax management and compliance, contained a major security vulnerability that affected employees at grocery giant Kroger and others.

34) As noted at the time by Brian Krebs, a respected American journalist and investigative reporter, "Equifax's W-2Express site makes electronic W-2 forms accessible for download for many companies, including Kroger — which employs more than 431,000 people. According to a letter Kroger sent to employees dated May 5, thieves were able to access W-2 data merely by entering at Equifax's portal the employee's default PIN code, which was nothing more than the last four digits of the employee's Social Security number and their four-digit birth year." (Brian Krebs, Crooks Grab W-2s from Credit Bureau Equifax, KREBS ON SECURITY, (May 6, 2016), https://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-creditbureau-equifax/ (September 10, 2017).

35) Krebs reported that in 2016 Equifax suffered at least three data breaches relating to its W-2 database alone. While Kroger was the largest, Krebs reported that earlier in the year, employees at Stanford University and Northwestern University also had their information breached via the W-2Express portal. *Id.*

36) The ramifications of Equifax's failure to protect the sensitive personal and tax information of its clients' employees are severe. Identity thieves can use the information stolen in the Data Breach to perpetrate a wide variety of crimes, including tax fraud, identity theft such as opening fraudulent credit cards and loan accounts, as well as various types of government fraud such as changing immigration status using the victim's name, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, obtaining a job, procuring housing, or even giving false information to police during an arrest. In the medical context, consumers' stolen Personal Information can be used to submit false insurance claims, obtain prescription drugs or medical devices for black-market resale, or get medical treatment in the victim's name.

37) The U.S. Social Security Administration (SSA) warns that "[i]dentity theft is one of the fastest growing crimes in America." (20 *Identity Theft And Your Social Security Number, Social Security Administration* (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf).

38) The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought." In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems." *Id.*

39) Under SSA policy, individuals cannot obtain a new Social Security number until there is evidence of ongoing problems due to misuse of the Social Security number. Even then, the SSA recognizes that "a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start." *Id.*

40) In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit." *Id.*

41) The processes of discovering and dealing with the repercussions of identity theft are time consuming and difficult. The Department of Justice's Bureau of Justice statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems." (Erika Harrell and Lynn Langton, *Victims of Identity Theft, 2012*, (Bureau of Justice Statistics), Dec. 2013, http://www.bjs.gov/content/pub/pdf/vit12.pdf.

42) Likewise, credit monitoring services are reactive not preventative, meaning they cannot catch identity theft until after it happens.

43) Additionally, there is some lag time between when harm occurs and when it is discovered, and also between when Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: *"law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."* (U.S. Government Accountability Office, GAO Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, http://www.gao.gov/new.items/d07737.pdf.

44) There is a very strong probability that Equifax victims are at imminent risk of further fraud and identity theft for years into the future. As a result of Equifax's negligent security practices and delay in notifying affected individuals, Plaintiffs and other Class members now face years of constant monitoring of their financial and personal accounts

and records to account for identity theft and fraud. Plaintiffs and Class members be faced with fraudulent debt, or incur costs for, among other things, paying monthly or annual fees for identity theft and credit monitoring services, obtaining credit reports, credit freezes, and other protective measures to deter, detect, and mitigate the risk of identity theft and fraud.

45) As a result of the compromising of their Personal Information, Plaintiffs and Class members have or may suffer one or a combination of the following injuries:

a. incidents of identity fraud and theft, including unauthorized bank activity,

b. fraudulent credit card purchases, and damage to their credit;

c. money and time expended to prevent, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of personal information;

d. lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach, including but not limited to efforts to research how to prevent, detect, contest, and recover from misuse of their personal information.

46) Furthermore, Plaintiffs and Class members have suffered, and/or will face an increased risk of suffering in the future, the following injuries:

a. money and time lost as a result of fraudulent access to and use of their financial accounts;

b. loss of use of and access to their financial accounts and/or credit;

c. impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

d. lowered credit scores resulting from credit inquiries following fraudulent activities;

e. costs and lost time obtaining credit reports in order to monitor their credit records;

f. money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;

g. money and time expended to avail themselves of assets and/or credit frozen or

flagged due to misuse;

h. costs of credit monitoring that is more robust than the services being offered by Equifax;

i. anticipated future costs from the purchase of credit monitoring and/or identity theft protection services;

j. costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;

k. money and time expended to ameliorate the consequences of the filing of fraudulent tax returns; and

l. continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Equifax fails to undertake appropriate, legally required steps to protect the personal information in its possession.

47) Ms. Domino, Mr. Almeida and Ms. Cejas hope Equifax will use this massive data breach, and their subsequent lawsuit, as a teachable moment to finally adopt adequate safeguards to protect against this type of cyberattack in the future.

CLASS ACTION ALLEGATIONS

48) Plaintiffs file this complaint as a national class action lawsuit. The Florida class consists of Florida consumers who:

a. Had personal or credit data collected and stored by Equifax in the past year, and

b. Who were subject to risk of data loss, credit harm, financial loss and identity theft or had to pay for third-party credit monitoring services as a result of Equifax's negligent data breach from May to July 2017.

49) Excluded from the class are all attorneys for the class, officers and members of Equifax, including officers and members of any entity with an ownership interest in Equifax, any judge who sits on the case, and all jurors and alternate jurors who sit on the case.

50) The exact number of aggrieved consumers in Florida can be determined based on Equifax's consumer database and the number of records breached, estimated at 8,084,000 consumers – about 43% of the population of Florida.

51) Every aggrieved Florida consumer suffered injuries as alleged in this complaint directly and proximately caused by Equifax's negligent failure to adequately protect its database from unauthorized access by third-party hackers.

52) **Numerosity. Fed. R. Civ. P. 23(a)(1).** The members of the class are so numerous and geographically dispersed that joinder of all members is impractical. While the exact number of Florida members is not known at this time, upon information and belief, the Florida class alone includes millions of consumers based on Equifax's estimate that its data breach affected 143 million consumers nationwide. Class members may be identified through objective means. Class members may be notified of this action by recognized, Court-approved notice dissemination methods, which may include U.S. Mail, electronic mail, internet postings, and/or published notices.

53) **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Fed. R. Civ. P. 23(a)(2) and 23(b)(3)'s predominance requirement, common questions of fact and law predominate over any questions affecting only individual class members. Common questions include

a. whether plaintiffs and the Florida class members are entitled to equitable relief;
b. whether Equifax acted negligently;
c. whether Equifax was negligent in failing to implement reasonable and accepted adequate security measures, procedures and practices;
d. whether plaintiffs and the Florida class members are entitled to recover money damages, among many others.

54) **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs' claims are typical of the claims of the Florida class because each suffered risk of loss, credit harm, identity theft and/or financial loss caused by Equifax's negligent failure to safeguard their data. The injuries suffered by plaintiffs and the Florida class members are identical (i.e. the costs to monitor and repair their credit through a third-party service for at least 24 months), and plaintiffs' claims for relief are based upon the same legal theories as are the claims of the other class members.

55) **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs are able to, have the ability to and will fairly and adequately protect and represent the interests of the class because their claims are typical of the claims of the Florida class, they are represented by respected attorneys who have experience handling complex litigation and consumer protection cases, who are qualified, competent and experienced, and who will vigorously prosecute this litigation, and their interests are not antagonistic or in conflict with the interests of the Florida class.

56) **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Fed. R. Civ. P. 23(b)(3), a class action is superior to other methods for fair and efficient adjudication of this case because common questions of law and fact predominate over other factors affecting only individual members, as far as plaintiffs know, no class action that purports to include Florida consumers suffering the same injury has been commenced in Florida, individual class members have little interest in controlling the litigation, due to the high cost of actions, the relatively small amounts of damages, and because plaintiffs and their attorneys will vigorously pursue the claims. The forum is desirable because the bulk of consumers in Florida who suffered injury caused by Equifax's negligence reside in the Southeast Florida area. A class action will be an efficient method of adjudicating the claims of the class members who have suffered relatively small damages, as a result of the same conduct by Equifax.

57) In the aggregate, class members have claims for relief that are significant in scope relative to the expense of litigation. The availability of defendant's consumer data will

facilitate proof of class claims, processing class claims, and distributions of any recoveries.

58) **Injunctive and Declaratory Relief.** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). Defendant, through its uniform conduct, has acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

59) Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Equifax failed to timely notify the public of the Data Breach;
b. Whether Equifax owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;
c. Whether Equifax's security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;
d. Whether Equifax failed to adequately comply with industry standards amounting to negligence;
e. Whether Defendant failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiffs and the Class members; and,
f. Whether adherence to data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

60) Finally, all members of the proposed Classes are readily ascertainable. Equifax has access to information regarding the Data Breach, the time period of the Data Breach, and which individuals were potentially affected. Using this information, the members of the Class can be identified and their contact information ascertained with relative ease for purposes of providing notice to the Class.

RETAIL DATA SECURITY STANDARDS

61) Although not exhaustive of adequate security measures that, due to the existential and ongoing threat, must be constantly evaluated and tested, the Payment Card Industry ("PCI") Data Security Standard provides an industry baseline for how retailers, wholesalers, banks and other business entities that store consumer data including names, social security numbers, credit card numbers, etc.

62) PIC standards are built a core set of security goals and have detailed instructions for compliance within each requirement. The 12 requirements and goals of PCI compliance are illustrated in the graphic below:

PCI Data Security Standard – High Level Overview

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

63) The fact that thieves were able to take the personal, credit and other information of millions of people who did not consent to or do any business with Equifax directly or indirectly shows a reckless disregard for the individual consumer's privacy and personal information.

CLAIM FOR RELIEF

Claim I

NEGLIGENCE

64) Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

65) As alleged in this complaint, defendant Equifax undertook care of credit and personal information belonging to plaintiffs and the Florida putative class, then breached its legal duty by failing to maintain adequate technological safeguards, falling below the standard of care for securing sensitive information in the technological industry, failing to update their software when they knew it was susceptible to hacking, directly and proximately causing foreseeable risk of data loss and credit harm and identity theft and other economic losses, in amounts to be decided by the jury.

66) Defendant Equifax knew their systems were prone to hacking and their data stores were at risk because of their lax data security and application "patching". Previously, starting on or about April 2016, thieves hacked Equifax systems and gained access to W-2 tax data of employees at client companies of Equifax's payroll subsidiary TALX. There have been a string of other data breaches as well which will shown in greater detail via discovery.

67) Defendant Equifax, to save money and increase profits, failed to update a critical piece of software, and hackers broke through using the older software's vulnerability, even though Equifax knew that an update to close a "security loophole" in the software was available and had been for several months prior to the data breach. According to an Equifax website press release, *"We know that criminals exploited a US website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638."* (Cybersecurity Incident & Important Consumer Information, www.equifaxsecurity2017.com, September 15, 2017). This flaw in the software had been fixed on March 6, 2017, and made available days later and updated at least once since then.

68) Defendant Equifax, willfully, knowingly and intentionally failed to update its Web applications despite demonstrable proof that the software "bug" gave real-world hackers an easy way to take control of sensitive sites and extract private and sensitive information.

69) But for defendant Equifax's failures to implement and maintain adequate security measures and update their software correctly and timely to protect consumer's personal information and credit records, Plaintiffs and Class Members would not be at a significantly heightened risk of identity theft, financial loss and fraud.

70) Plaintiffs and Class Members seek compensatory and punitive damages with interest, the costs of suit and attorney's fees, and all other and further relief as this Court deems just and proper.

Claim II

NEGLIGENCE *Per Se*

71) Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

72) As set forth above, Equifax is required under the Fair Credit Reporting Act, 15 U.S.C. §§ 1681e, to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

73) Equifax failed to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA.

74) Plaintiffs and Class members were foreseeable victims of Equifax's violation of the FCRA. Equifax knew or should have known that a breach of its data security systems would cause damages to Class members.

75) Equifax was also required under the Gramm-Leach-Bliley Act ("GLBA") to satisfy certain standards relating to administrative, technical, and physical safeguards: "(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." 15 U.S.C. § 6801(b).

76) In order to satisfy their obligations under the GLBA, Equifax was also required to "develop, implement, and maintain a comprehensive information security program that is (1) written in one or more readily accessible parts, and (2) contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.4.

77) In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id.*

78) Further, when Equifax became aware of "unauthorized access to sensitive customer information," it should have "conduct[ed] a reasonable investigation to promptly determine the likelihood that the information has been or will be misused" and "notif[ied] the affected customer[s] as soon as possible." *Id.*

79) Equifax violated by GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Equifax's failure to implement and maintain adequate data security practices to safeguard Class members' Personal Information; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendants' data

security practices were inadequate to safeguard Class members' Personal Information. 107. Equifax also violated the GLBA by failing to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." This includes, but is not limited to, Equifax's failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

80) Equifax also violated by the GLBA by failing to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer information. 109. Plaintiffs and Class members were foreseeable victims of Equifax's violation of the FCRA. Equifax knew or should have known that a breach of its data security systems would cause damages to Class members.

81) Likewise, Section 5 of the FTC Act prohibits "*unfair . . . practices in or affecting commerce,*" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect Personal Information. The FTC publications and orders described above also form part of the basis of Equifax's duty in this regard.

82) Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards, as described in detail herein. Equifax's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored, and the foreseeable consequences of a data breach at a corporation such as Equifax, including, specifically, the immense damages that would result to Plaintiffs and Class members.

83) Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

84) Equifax's failure to comply with the applicable laws and regulations, including the FCRA, the GLBA, and the FTC Act constitutes negligence *per se*.

85) But for Equifax's violation of the applicable laws and regulations, Class members' Personal Information would not have been accessed by unauthorized individuals.

86) As a result of Equifax's failure to comply with applicable laws and regulations, Plaintiffs and Class members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs and Class members' Personal Information has also diminished the value of the Personal Information.

87) The damages to Plaintiffs and the Class members were a proximate, reasonably foreseeable result of Equifax's breaches of it's the applicable laws and regulations.

88) Plaintiffs and Class Members seek compensatory and punitive damages with interest, the costs of suit and attorney's fees, and all other and further relief as this Court deems just and proper.

89) Equifax violated by GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Equifax's failure to implement and maintain adequate data security practices to safeguard Class members' Personal Information; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class members' Personal Information.

90) Equifax also violated the GLBA by failing to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." This includes, but is not limited to, Equifax's failure to

notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

91) Equifax also violated by the GLBA by failing to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer information. 109. Plaintiffs and Class members were foreseeable victims of Equifax's violation of the FCRA. Equifax knew or should have known that a breach of its data security systems would cause damages to Class members.

92) Likewise, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect Personal Information. The FTC publications and orders described above also form part of the basis of Equifax's duty in this regard.

93) Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards, as described in detail herein. Equifax's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored, and the foreseeable consequences of a data breach at a corporation such as Equifax, including, specifically, the immense damages that would result to Plaintiffs and Class members.

94) Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

95) Equifax's failure to comply with the applicable laws and regulations, including the FCRA, the GLBA, and the FTC Act constitutes negligence *per se*.

96) But for Equifax's violation of the applicable laws and regulations, Class members' Personal Information would not have been accessed by unauthorized individuals. 115. As a result of Equifax's failure to comply with applicable laws and regulations,

Plaintiffs and Class members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft.

97) Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft.

98) The unauthorized acquisition of Plaintiffs and Class members' Personal Information has also diminished the value of the Personal Information.

99) The damages to Plaintiffs and the Class members were a proximate, reasonably foreseeable result of Equifax's breaches of it's the applicable laws and regulations.

100) Therefore, Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

Claim III

VIOLATION OF THE FAIR CREDIT REPORTING ACT

101) Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

102) As individuals, Plaintiffs and Class member are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

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

104) Equifax is a consumer reporting agency under the FCRA because, for monetary fees, 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.

105) As a consumer reporting agency, the FCRA requires Equifax to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. §1681e(a).

106) Under the FCRA, a "consumer report" is defined as "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 -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1).

107) The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class members' eligibility for credit.

108) As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed the Nationwide Class members' Personal Information. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer

hackers, as detailed above.

109) Equifax furnished the Nationwide Class members' consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

110) The Federal Trade Commission ("FTC") has pursued enforcement actions against consumer reporting agencies under the FCRA for failing to "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches. Statement of Commissioner Brill (Federal Trade Commission 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819settlementonestatement.pdf

111) Equifax willfully and/or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. The willful and reckless nature of Equifax's violations is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

112) 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. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary on The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix to Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiffs and other members of the classes of their rights under the FCRA.

113) Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and Nationwide Class members' Personal Information for no permissible purposes under the FCRA.

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

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

Claim IV

BREACH OF IMPLIED CONTRACT

116) Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

117) Plaintiffs and many Class members entered into an implied contract with Equifax whereby consumers paid money and provided their Personal Information to Equifax in exchange for credit reporting services.

118) As part of this transaction, Plaintiffs' and Class members entered into implied contracts with Equifax pursuant to which Equifax agreed to safeguard and protect such Personal Information and to timely and accurately notify consumers if their data had been breached and compromised.

119) In entering into such implied contracts, Plaintiffs and Class members assumed that Equifax's data security practices and policies were reasonable and consistent with industry standards, and that Equifax would use part of the funds received from Plaintiffs and the Class members to pay for adequate and reasonable data security practices.

120) Plaintiffs and Class members would not have provided and entrusted their Personal Information to Equifax in the absence of the implied contract between them and Equifax to keep the information secure.

121) Plaintiffs and Class members fully performed their obligations under the implied contracts with Equifax.

122) Equifax breached its implied contracts with Plaintiffs and Class members by failing to safeguard and protect their Personal Information and by failing to provide timely and accurate notice that their Personal Information was compromised as a result of the Data Breach.

123) As a direct and proximate result of Equifax's breaches of the implied contracts, Plaintiffs and Class members sustained actual losses and damages as described herein.

124) Plaintiffs and Class Members seek compensatory and punitive damages with interest, the costs of suit and attorney's fees, and all other and further relief as this Court deems just and proper.

COUNT V

UNJUST ENRICHMENT

125) Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

126) Plaintiffs and the Class conferred a monetary benefit on Equifax as Equifax traded on and sold consumers' Personal Information in the form of credit reports and by other means in order to generate significant revenue for Equifax.

127) Equifax appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and the Class.

128) The revenue generated by Equifax should have been used by Equifax, in part, to pay for the costs of reasonable data privacy and security practices and procedures.

129) Under principles of equity and good conscience, Equifax should not be permitted to retain the money belonging to Plaintiffs and Class members because Equifax failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and class members paid for wither knowingly or unknowingly.

130) Equifax should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful or inequitable proceeds received by it. A constructive trust should be imposed upon all unlawful or inequitable sums received by Equifax traceable to Plaintiffs and Class members.

131) Plaintiffs and Class Members seek compensatory and punitive damages with interest, the costs of suit and attorney's fees, and all other and further relief as this Court deems just and proper.

COUNT VI

VIOLATION OF FLORIDA's INFORMATION PROTECTION ACT OF 2014
FLORIDA STATUTE 501.171 ("FIPA")

132) Plaintiffs incorporate all prior paragraphs as though fully set forth herein.

133) Defendant Equifax violated § 501.171, Florida Statutes (2017), also called the "Florida Information Protection Act", or "FIPA", of 2014. FIPA says, *"An act relating to security of confidential personal information; providing a short title; repealing s. 4 817.5681, F.S., relating to a breach of security concerning confidential personal information in third-party possession, creating s. 501.171, F.S.; providing definitions; requiring specified entities to take reasonable measures to protect and secure data containing personal information in electronic form; requiring specified entities to notify the Department of Legal Affairs of data security breaches; requiring notice to individuals of data security breaches under certain circumstances..."*

134) Having been signed into law on June 20, 2014, by Governor Rick Scott, this new law replaced Florida's prior data breach notification statute, § 817.5681, Florida Statutes. This new statute made several significant modifications and enhancements to Florida law that affects businesses, government and other entities not just on Florida, but beyond its borders as well.

135) Defendant Equifax is a "covered entity" as defined in §501.171(b), Florida Statutes. As a "covered entity", Defendant Equifax was and is required to meet certain security standards pursuant to §501.171(2), Florida Statutes, which states, *"Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information."*

136) Defendant Equifax violated §501.171(3)(a), Florida Statutes, in that it failed to notify the department of any breach of security affecting 500 or more individuals in this state. Such notice was required within 30 days of discovery of the breach, along with a synopsis of what occurred. "*A covered entity shall provide notice to the department of any breach of*

security affecting 500 or more individuals in this state. Such notice must be provided to the department as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach occurred."

(b) The written notice to the department must include:

1. A synopsis of the events surrounding the breach at the time notice is provided.

137) Under FIPA, personal information includes an individual's first name or first initial combined with the individual's last name, in combination with social security number, driver's license number or other similar number of a government-issued ID, or a financial account number or credit or debit card number combined with the required security code. New under FIPA, personal information also will include any information about an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional; or an individual's health insurance policy number or subscriber identification number, along with any unique identifier used by a health insurer to identify the individual.

138) FIPA also expands the definition of personal information to include any personal login information that would permit access to a person's online account. Notably, this expansion, which may be the first of its kind in any state data breach notification law, would include login information to social media sites or applications, regardless of whether such sites include more traditional forms of personal information.

139) FIPA reduced the time period for report of breaches to 30 days from the time the breach is discovered, down from 45 days under the previous Florida statute. FIPA authorizes the Department of Legal Affairs to grant up to 15 additional days to provide notice if good cause is provided in writing to the department within 30 days of the determination of a breach.

140) If the breach affects 500 or more persons, FIPA requires that notice also be provided to the Florida Department of Legal Affairs. If the breach affects 1,000 or more persons, additional notice must be given to all nationwide consumer credit reporting agencies. Defendant Equifax willfully failed to do either.

141) As a direct and proximate result of defendant Equifax's actions or inactions, Plaintiffs and Class Members seek compensatory and punitive damages with interest, the costs of suit and attorney's fees, and all other and further relief as this Court deems just and proper.

CLASS

142) Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of themselves and those similarly situated, the classes which can be preliminarily defined as follows:

Nationwide Class

All consumers in the United States whose personal information was compromised as a result of the data breach announced by Equifax in September 2017.

Florida Class

All consumers residing in Florida whose personal information was compromised as a result of the data breach announced by Equifax in September 2017.

143) Plaintiffs and all class members are entitled to equitable relief in the form of an accounting of exactly how their credit and personal information was accessed without authorization by third parties, restitution, and unless agreed upon by Equifax, an order to preserve all documents and information (and electronically stored information) pertaining to this case.

144) Plaintiffs satisfy the numerosity, commonality, typicality and adequacy prerequisites for suing as a representative party pursuant to Rule 23.

PRAYER FOR RELIEF

Plaintiffs seek relief for themselves and the proposed Florida Class as follows:

a. Unless agreed upon by Equifax, an order to preserve all documents and information (and electronically stored information) pertaining to this case,
b. An order certifying this matter as a class action,

c. Judgment against Equifax for fair compensation in an amount to be decided by the jury, plus costs, and

d. All other relief the Court deems necessary, proper and just.

JURY TRIAL DEMANDED

Plaintiffs and the Class members hereby demand a trial by jury.

Date: September 29, 2017.

Respectfully submitted,

/s/ Alex F. Arreaza
Alex F. Arreaza, Esq.
Florida Bar No. 0001783
Attorney for Plaintiffs
THE ARREAZA LAW FIRM, LLC
320 W. Oakland Park Blvd.
Wilton Manors, FL 33311
Office: 954-565-7743
Fax: 954-565-7713
Email: alex@alexmylawyer.com

/s/ Joseph Zager
Joseph Zager, Esq.
Florida Bar No. 163491
Of Attorney for Plaintiffs
ZAGERLAW, P.A.
500 E. Broward Blvd., Suite 1820
Fort Lauderdale, FL 33394
Office: 954-888-8170
Email: joseph@zagerlaw.com

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

BARBARA J. DOMINO, DANIEL E. ALMEIDA and MIRIAM CEJAS

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

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

Alex Arreaza, 320 W Oakland Park Blvd., Wilton Manors, FL 33311
Joseph Zager, 500 E. Broward Blvd, Ste 1820, Ft Lauderdale, FL 33394

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. Negligence, Violation of the FCRA, Breach of Implied Contract, Unjust Enrichment

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 September 29, 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

BARBARA J. DOMINO,
DANIEL E. ALMEIDA and
MIRIAM CEJAS,

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
THE PRENTICE HALL CORPORATION SYSTEM, INC.
1201 HAYS STREET, SUITE 105
TALLAHASSEE, FL 32301

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: ALEX ARREAZA, ESQ.
THE ARREAZA LAW FIRM, LLC
320 W. OAKLAND PARK BLVD
WILTON MANORS, FL 33311

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: