UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
MIAMI DIVISION

JACQUELINE MARTINEZ, and
BARRON A. LIBASCI, on behalf of themselves
and all others similarly situated,

Plaintiff,

v.

EQUIFAX, INC.,

Defendant.
_____/

CASE NO. _____

CLASS ACTION

CLASS ACTION COMPLAINT

Plaintiffs Jacqueline Martinez and Barron A. Libasci (hereinafter, "Plaintiffs"), individually and on behalf of the Classes defined below, allege the following against Equifax, Inc. ("Equifax") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of publicly available documents as to all other matters:

INTRODUCTION

1. Plaintiffs bring this class action case against Equifax for its gross and systemic failures to secure and safeguard consumers' personally identifiable information ("PII") which Equifax collected from various sources in connection with the operation of its business as a consumer credit reporting agency, and for failing to provide timely, accurate and adequate notice to Plaintiffs and other Class members that their PII had been stolen and precisely what types of information were stolen.

2. Equifax has acknowledged that a cybersecurity incident ("Data Breach")

potentially impacting approximately 143 million U.S. consumers occurred. It has also acknowledged that unauthorized persons exploited a U.S. website application vulnerability to gain access to certain files. Equifax claims that based on its investigation, the unauthorized access occurred from mid-May through July 2017. By Equifax's own admission, the information accessed primarily includes names, Social Security numbers, birth dates, addresses and some driver's license numbers. Equifax has also confirmed that 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 stolen.

3. Equifax learned of the Data Breach on July 29 2017, but failed to disclose it to affected consumers and the public at large until September 7, 2017. Instead, three senior Equifax executives sold at least $1.8 million worth of shares before the public disclosure of the breach.

4. The PII for Plaintiffs and the class of consumers they seek to represent was compromised due to Equifax's acts and omissions and their failure to properly protect the PII.

5. Equifax could have prevented this Data Breach. Data breaches at other companies, including one of its major competitors, Experian have occurred.

6. The Data Breach was the inevitable result of Equifax's inadequate approach to data security and the protection of the PII that it collected during the course of its business.

7. Equifax disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and security practices to safeguard PII, failing to take available steps to prevent and stop the breach from ever happening, and failing to monitor and detect the breach on a timely basis.

8. As a result of the Equifax Data Breach, the PII of the Plaintiffs and Class members has been exposed to criminals for misuse. The injuries suffered by Plaintiffs and Class members, or likely to be suffered by Plaintiffs and Class members as a direct and proximate result of the Equifax Data Breach include: (a) theft of their personal and financial information; (b) costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach; (d) the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their personal and financial information being placed in the hands of hackers; (e) damages to, and diminution in value of, their personal and financial information entrusted to Equifax for the sole purpose of Equifax's credit-reporting services and with the mutual understanding that Equifax would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others; (f) money paid to Equifax for credit-reporting services during the period of the Data Breach in that Plaintiffs and Class members would not have obtained, or permitted others to obtain, Equifax's credit-reporting services had Equifax disclosed that it lacked adequate systems and procedures to reasonably safeguard consumers' financial and personal information and had Equifax provided timely and accurate notice of the Data Breach; (g) overpayments paid to Equifax for credit-reporting services in that a portion of the price paid by Plaintiffs and the Class, or others on their behalf, to Equifax was for the costs of Equifax

providing reasonable and adequate safeguards and security measures to protect customers' financial and personal data, which Equifax did not do, and as a result, Plaintiffs and members of the Class did not receive what was paid for and Equifax overcharged for these services; and (h) continued risk to their financial and personal information, which remains in the possession of Equifax and which is subject to further breaches so long as Equifax fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' PII in its possession.

9. The injuries to the Plaintiffs and Class members were directly and proximately caused by Equifax's failure to implement or maintain adequate data security measures for PII.

10. Further, Plaintiffs retain a significant interest in ensuring that their PII, which, while stolen, remains in the possession of Equifax is protected from further breaches, and seek to remedy the harms they have suffered on behalf of themselves and similarly situated consumers whose PII was stolen as a result of the Equifax Data Breach.

11. Plaintiffs bring this action to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiffs seek the following remedies, among others: statutory damages under the Fair Credit Reporting Act ("FCRA") and state consumer protection statutes, reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to implement improved data security measures.

JURISDICTION AND VENUE

12. This Court has federal question jurisdiction under 28 U.S.C. § 1331 based on the Fair Credit Reporting Act claims alleged herein, and supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367. Alternatively, this Court has subject matter jurisdiction over this

action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because the amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 putative class members, and many members of the proposed Classes are citizens of states different from Equifax.

13. This Court has personal jurisdiction over Equifax because Equifax regularly conducts business in Florida, and has sufficient minimum contacts in Florida. Equifax intentionally availed itself of this jurisdiction by marketing and selling products and services and by accepting and processing payments for those products and services within Florida.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Equifax regularly transacts business in this District, and hundreds of thousands of the Class members, including Plaintiffs, reside in this District. The cause of actions for hundreds of thousands of putative class members also arose, in part, in this District.

PARTIES

15. Plaintiff Jacqueline Martinez resides in Miami-Dade County, Florida, and is a Florida citizen. Following the disclosure of the Data Breach, Martinez accessed Equifax's website, www.trustedidpremier.com, inputting her last name and six digits from her social security number as instructed, and received a response indicating that Equifax believes her personal information was impacted by the Data Breach.

16. Plaintiff Barron Libasci resides in Miami-Dade County, Florida, and is a Florida citizen. Following the disclosure of the Data Breach, Libasci accessed Equifax's website, www.trustedidpremier.com, inputting his last name and six digits from his social security number as instructed, and received a response indicating that Equifax believes his personal information was impacted by the Data Breach.

17. Plaintiffs' personal and financial information was compromised as a result of Equifax's failures and gross misconduct that resulted in the Data Breach. Plaintiffs were harmed and sustained actual, concrete damages by having their financial and personal information compromised by the Data Breach.

18. Plaintiffs would not have provided, or would not have authorized others to provide, their personal and financial information to Equifax in connection with credit-reporting services had Equifax disclosed that it lacked adequate computer systems and data security practices to safeguard consumers' personal and financial information from hacking and theft.

19. Plaintiffs suffered actual and concrete injury as a result of Equifax's systemic failures and gross misconduct that resulted in the Data Breach.

20. Defendant Equifax, Inc. is a Delaware corporation with its principal place of business located in Atlanta, Georgia. It provides credit information services to millions of business, governmental units, and consumers throughout the world. Equifax operates through various subsidiaries and agents, each of which entities acted as agents of Equifax, or in the alternative, in concert with Equifax.

CLASS ACTION ALLEGATIONS

21. Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated.

A. Nationwide Class

22. Plaintiffs assert statutory claims under the Fair Credit Reporting Act and common law claims for negligence on behalf of all U.S. consumers defined as follows:

> All persons residing in the United States whose personally identifiable information (PII) was accessed, compromised, or acquired by unauthorized persons in the Equifax Data Breach first disclosed on or about September 7, 2017 (the "Nationwide Class").

B. Statewide Classes

23. Plaintiffs assert statutory claims under the laws of various individual states, and on behalf of separate statewide classes, defined as follows:

> All persons residing in [STATE] whose PII was accessed, compromised, or acquired by unauthorized persons in the Equifax Data Breach first disclosed on or about September 7, 2017 (the "Statewide Classes").

C. Florida Subclass

24. Plaintiffs also assert a statutory claim under the Florida Deceptive and Unfair Trade Practices Act on behalf of all Florida consumers defined as follows:

> All persons residing in Florida whose PII was accessed, compromised, or acquired by unauthorized persons in the Equifax Data Breach first disclosed on or about September 7, 2017 (the "Florida Subclass").

25. Excluded from the Nationwide Class, the Statewide Classes, and the Florida Subclass (collectively, the "Classes") are Equifax, its affiliates, parents or subsidiaries, its officers, directors and members of their immediate families and any entity in which Equifax has a controlling interest, the legal representatives, heirs, successors or assigns of any such excluded party, all persons who make a timely election to be excluded from the Class, government entities; and the judicial officer(s) to whom this case is assigned, and the members of their immediate families.

26. Plaintiffs reserve the right to amend or modify the definition of the proposed Classes if necessary after having had an opportunity to conduct discovery.

27. Each of the proposed Classes meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3).

28. ***Numerosity. Fed. R. Civ. P. 23(a)(1).*** The members of the Class are so numerous that the joinder of each member is impractical. By Equifax's own admission, the Classes consist

of approximately 143 million members, the identity of whom are well within the knowledge of and can be ascertained by resort to Equifax's records. In fact, Equifax's www.trustedidpremier.com website already maintains the identities of these class members, demonstrating Equifax has the administrative capability through its computer systems and other records to identify all members of the Classes, and such specific information is not otherwise available to Plaintiffs.

29. ***Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).*** Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

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

b. Whether Equifax owed a duty to Plaintiffs and members of the Classes to adequately protect their PII;

c. Whether Equifax owed a duty to Plaintiffs and members of the Classes to provide timely and accurate notice of the Data Breach to Plaintiffs and members of the Classes;

d. Whether Equifax breached its duty to Plaintiffs and members of the Classes by failing to provide adequate data security;

e. Whether Equifax breached its duty to Plaintiffs and members of the Classes by failing to provide timely and accurate notice of the Data Breach to Plaintiffs and members of the Classes;

f. Whether Equifax knew or should have known that their data security systems were highly vulnerable to attack;

g. Whether Equifax unlawfully failed to disclose that it did not maintain computers and security practices adequate to reasonably safeguard consumers' financial and personal data;

h. Whether Equifax's security measures to protect their systems were reasonable in light of the measures recommended by data security experts;

i. Whether Equifax was negligent in failing to implement reasonable and adequate security procedures and practices;

j. Whether Equifax's failure to implement adequate data security measures allowed the breach to occur;

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

l. Whether Equifax's conduct, including their failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiffs and members of the Classes;

m. Whether Plaintiffs and members of the Classes suffered injured, including ascertainable losses, as a result of Equifax's conduct (or failure to act);

n. Whether Plaintiffs and members of the Classes are entitled to recover monetary relief; and

o. Whether Plaintiffs and members of the Classes are entitled to equitable relief, including declaratory and injunctive relief, restitution, disgorgement, and/or other equitable relief.

30. ***Typicality. Fed. R. Civ. P. 23(a)(3).*** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs' claims are typical of those of other Class members. Plaintiffs had their PII compromised in the Data Breach. Plaintiffs' damages and injuries are akin to other Class members and Plaintiffs seek relief consistent with the relief of the Class.

31. ***Adequacy. Fed. R. Civ. P. 23(a)(4).*** Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Equifax to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class and have retained competent counsel experienced in the prosecution of class actions. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class' interests.

32. ***Superiority. Fed. R. Civ. P. 23(b)(3).*** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers

even when damages to individual Plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Equifax, and thus, individual litigation to redress Equifax's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

33. ***Injunctive and Declaratory Relief. Fed. R. Civ. P. 23(b)(2) and (c).*** The requirements of Fed. R. Civ. P. 23(b)(2) and (c) are also met because Equifax, through its uniform conduct, has acted or refused to act on grounds generally applicable to the Classes, making injunctive and declaratory relief appropriate for the Classes as a whole.

STATEMENT OF FACTS

34. Equifax is one of three nationwide credit-reporting companies that tracks and rates the financial history of U.S. consumers. The companies are supplied with data about loans, loan payments and credit cards, as well as information on everything from child support payments, credit limits, missed rent and utilities payments, addresses and employer history. All of this information, and more, factors into consumers' credit scores.

35. Unlike other data breaches, not all of the people affected by the Equifax breach may be aware that they are customers of the company. Equifax gets its data from credit card companies, banks, retailers, and lenders who report on the credit activity of individuals to credit reporting agencies, as well as by purchasing public records.

36. According to Equifax's report on September 7, 2017, the breach was discovered on July 29th. The perpetrators gained access by "[exploiting] a [...] website application vulnerability" on one of the company's U.S.-based servers. The hackers were then able to "gain access to certain files." See https://www.equifaxsecurity2017.com/ (last visited September 22, 2017).

37. Included among those files was a treasure trove of personal data: names, dates of birth, Social Security numbers and addresses. In some cases -- Equifax states around 209,000 -- the records also included actual credit card numbers. Documentation about disputed charges was also leaked. Those documents contained additional personal information on around 182,000 Americans.

38. Personal data like this is a major score for cybercriminals who will likely look to capitalize on it by launching targeted phishing campaigns.

39. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their PII – a form of intangible property that Plaintiffs entrusted to Equifax and that was compromised in and as a result of the Equifax Data Breach.

40. Additionally, Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by their PII being placed in the hands of criminals who have already, or will imminently, misuse such information.

41. Moreover, Plaintiffs have a continuing interest in ensuring that their private information, which remains in the possession of Equifax, is protected and safeguarded from future breaches.

42. At all relevant times, Equifax knew, or reasonably should have known, that the PII it collected, maintained and stored is highly sensitive, susceptible to attack, and could be used

for wrongful purposes by third parties, such as identity theft and fraud.

43. Equifax recognized its obligation to maintain the security of U.S. consumers' PII and financial information in its Privacy Policy:

> 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

See http://www.equifax.com/privacy/ (last visited September 22, 2017).

44. Equifax further promises to consumers that "[w]e will not disclose your personal information to third parties except to provide you with the disclosure or service you request . . ." *See* http://www.equifax.com/privacy/personal-credit-reports (last visited September 22, 2017). Equifax also promises that it is "committed to protecting the security of your information through procedures and technology designed for this purpose." *Id*.

45. It is well known and the subject of many media reports that PII is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate entities, including Experian, Equifax maintained an insufficient and inadequate system to protect the PII of Plaintiffs and Class members.

46. Although Equifax claims to be a leader in data security and its privacy policy promises to reasonably safeguard consumer data, Equifax's own data security practices were inadequate. Equifax was well aware of this fact because it had experienced multiple data breaches in recent years.

47. In March 2014, Equifax reported a data breach to the New Hampshire Attorney

General involving an IP address operator who was able to obtain Equifax consumer credit reports using sufficient personal information to bypass Equifax's identity verification process. *See* Letter from Troy G. Kubes, Vice President & Associate Group Counsel at Equifax Legal Department, to Attorney General Joseph Foster, March 5, 2014, https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20140305.pdf (last visited September 22, 2017).

48. In May 2016, Equifax's W-2 Express website suffered a data breach where an attacker was able to access, download and post the names, addresses, social security numbers and other personal information of over 430,000 Kroger employees. The attackers were able to access the W-2 data by merely entering Equifax's portal with an employee's default PIN code, which was the last four digits of the employee's Social Security number and their four-digit birth year. *See* Crooks Grab W-2s from Credit Bureau Equifax, Krebs on Security, http://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/ (last visited September 22, 2017).

49. Independent security researchers have also found that Equifax's website is vulnerable. In 2016, a security researcher found a common vulnerability known as cross-site scripting (XSS) on the main Equifax website. Such XSS bugs allow attackers to send specially-crafted links to Equifax customers and, if the target clicks through and is logged into the site, their username and password can be revealed to the hacker. *See* A Brief History of Equifax Security Fails, Forbes, https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#53a60715677c (last visited September 22, 2017).

50. Researcher Kenneth White just recently discovered a link in the source code on the Equifax consumer sign-in page that pointed to Netscape, a web browser that was

discontinued in 2008. Kevin Beaumont, a British security professional, found decade-old software in use, including IBM WebSphere, Apache Struts and Java, many of which are outdated and subject to well-known vulnerabilities. *Id.*

51. Given its critical role in credit markets, and the vast amounts of the most detailed PII and financial information of U.S. consumers that can be easily used by hackers or customers of hackers to prey on innocent consumers by using their identities and credit, Equifax was aware of the need to have the most current protective measures in place to prevent a hack and to minimize the impact of a hack should an intrusion occur. It is incomprehensible that Equifax had such poor protections and systems in place to allow hackers to infiltrate the PII and financial information of 143 million U.S. consumers for well over a month before being detected.

52. On September 13, 2017, Equifax confirmed that there was a vulnerability in its systems called Apache Struts CV-2017-5638. *See* https://www.equifaxsecurity2017.com/ (last visited on September 22, 2017). According to the Apache Software Foundation, the software company that Equifax used to build the website that was hacked, the Data Breach occurred due to Equifax's failure to install security updates to a server that it received from Apache in a timely manner. See https://blogs.apache.org/foundation/date/20170914 (last visited on September 25, 2017). That vulnerability was well known to Equifax in early March 2017, when a security patch was issued. Yet, shockingly, Equifax failed to install the patch, leaving its web server unsecure.

53. PII is a valuable commodity because it contains not only payment card numbers but PII as well. A "cyber blackmarket" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. PII is "as good as gold" to identity thieves because they can use

victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

54. Social Security numbers are a particularly popular target for hackers. Combinations of Social Security numbers, birth dates and names sell for more than credit card numbers in an increasingly sophisticated black market, where such information is sold and resold through popular auction sites.

55. Legitimate organizations and the criminal underground alike recognize the value in PII contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users." *See* Verizon 2014 PCI Compliance Report, available at: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 (last visited September 20, 2017).

56. At all relevant times, Equifax knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

57. Equifax was, or should have been, fully aware of the significant number of people whose PII it collected, and thus, the significant number of individuals who would be harmed by a breach of Equifax's systems.

58. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, Equifax's approach to maintaining the privacy and security of the PII of Plaintiffs and Class members was

lackadaisical, cavalier, reckless, or at the very least, negligent.

59. The ramifications of Equifax's failure to keep Plaintiffs' and Class members' data secure are severe.

60. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R § 248.201 (2013). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person." *Id*.

61. Personal identifying information (PII) is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance." Federal Trade Commission, Warning Signs of Identity Theft, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited September 20, 2017).

62. Identity thieves can use personal information, such as that of Plaintiffs and Class members which Equifax failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; 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; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

63. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years. *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited September 20, 2017).

64. Reimbursing a consumer for a financial loss due to fraud does not make that

individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014. Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited September 20, 2017).

65. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw 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.

GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited September 20, 2017)

66. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

67. The PII of Plaintiffs and Class members is private and sensitive in nature and was left inadequately protected by Equifax. Equifax did not obtain Plaintiffs' and Class members' consent to disclose their PII to any other person as required by applicable law and industry standards.

68. The Equifax Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiffs' and Class members' PII from unauthorized access, use,

and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

69. Equifax had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

70. Had Equifax remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Equifax would have prevented the Data Breach and, ultimately, the theft of its customers' PII.

71. As a direct and proximate result of Equifax's wrongful actions and inaction and the resulting Data Breach, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a credit reporting agency's slippage, as is the case here.

72. Equifax's wrongful actions and inaction directly and proximately caused the theft

and dissemination into the public domain of Plaintiffs' and Class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Theft of their personal and financial information;

b. Unauthorized charges on their debit and credit card accounts;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the black market;

d. The untimely and inadequate notification of the Data Breach;

e. The improper disclosure of their PII;

f. Loss of privacy;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;

i. Ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

j. Loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

k. The loss of productivity and value of their time spent to address attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

73. Equifax has not offered customers any meaningful credit monitoring or identity

theft protection services, despite the fact that it is well known and acknowledged by the government that damage and fraud from a data breach can take years to occur. As a result, Plaintiffs and Class members are left to their own actions to protect themselves from the financial damage Equifax has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Equifax's actions have created for Plaintiffs and Class members, is ascertainable and is a determination appropriate for the trier of fact. Equifax has also not offered to cover any of the damages sustained by Plaintiffs or Class members.

74. Experts are now recommending that all Americans whose PII is impacted by the Data Breach should freeze their credit with all three of the major credit reporting agencies, Equifax, Experian, and TransUnion. There are financial costs associated with freezing and unfreezing a consumer's credit report, further compounding the actual and concrete damages that Plaintiffs and the Classes have and will sustain. Even if a less onerous lock is placed on the credit report, members of the Classes have been advised to regularly monitor activity on their credit reports to determine whether any nefarious conduct has occurred which would require a locking of their credit. *See* https://www.transunion.com/credit-freeze/place-credit-freeze2 (last visited September 22, 2017).

75. While the PII of Plaintiffs and members of the Class has been stolen, Equifax continues to hold PII of consumers, including Plaintiffs and Class members. Particularly because Equifax and has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiffs and members of the Class have an undeniable interest in insuring that their PII is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

COUNT I
WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)

76. Plaintiffs restate and reallege Paragraphs 1 through 75 as if fully set forth here.

77. This is a claim for relief under the Fair Credit Reporting Act ("FRCA"), 11 U.S.C. § 1681, *et seq.*

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

79. 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).

80. 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 to furnish consumer reports to third parties evaluating the consumers' credit for varying purposes.

81. 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).

82. 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).

83. 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.

84. 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).

85. 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' PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

86. 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.

87. 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.

88. 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.

89. 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 members of the Nationwide Class of their rights under the FCRA.

90. Equifax's willful and/or reckless conduct provided a means for unauthorized

intruders to obtain and misuse Plaintiffs' and members of Nationwide Class members' personal information for no permissible purposes under the FCRA.

91. Plaintiffs and members of the Nationwide Class have been damaged by Equifax's willful or reckless failure to comply with the FCRA.

92. Plaintiffs and members of the Nationwide Class are therefore 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).

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

COUNT II
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)

94. Plaintiffs restate and reallege Paragraphs 1 through 75 and 77 through 87 as if fully set forth herein.

95. This is a claim for relief under the Fair Credit Reporting Act ("FRCA"), 11 U.S.C. § 1681, *et seq*.

96. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA.

97. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and the Nationwide Class members' PII and consumer reports for no permissible purposes under the FCRA.

98. Plaintiffs and the Nationwide Class members have been damaged by Equifax's negligent failure to comply with the FCRA.

99. Plaintiffs and each of the Nationwide Class members are therefore entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

100. Plaintiffs and the Nationwide Class members are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT III
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)

101. Plaintiffs restate and reallege Paragraphs 1 through 75 as if fully set forth herein.

102. This is a claim for relief based on common law negligence.

103. Upon accepting and storing the PII of Plaintiffs and members of the Nationwide Class in its computer systems and on its networks, Equifax undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Equifax knew that the PII was private and confidential and should be protected as private and confidential.

104. Equifax owed a duty of care not to subject Plaintiffs, along with their PII, and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

105. Equifax owed numerous duties to Plaintiffs and to members of the Nationwide Class, including the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b. To protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

106. Equifax also breached its duty to Plaintiffs and the Class members to adequately

protect and safeguard PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering their dilatory practices, Equifax failed to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiffs and Class members, misuse the PII and intentionally disclose it to others without consent.

107. Equifax knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Equifax knew about numerous, well-publicized data breaches, including the breach at Experian.

108. Equifax knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class members' PII.

109. Equifax breached its duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiffs and Class members.

110. Because Equifax knew that a breach of its systems would damage millions of individuals, including Plaintiffs and Class members, Equifax had a duty to adequately protect their data systems and the PII contained thereon.

111. Equifax had a special relationship with Plaintiffs and Class members. Plaintiffs' and Class members' willingness to entrust Equifax with their PII was predicated on the understanding that Equifax would take adequate security precautions. Moreover, only Equifax had the ability to protect its systems and the PII it stored on them from attack.

112. Equifax's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their PII. Equifax's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

113. Equifax also had independent duties under state and federal laws that required Equifax to reasonably safeguard Plaintiffs' and Class members' Personal Information and promptly notify them about the data breach.

114. Equifax breached its duties to Plaintiffs and Class members in numerous ways, including:

a. By failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiffs and Class members;

b. By creating a foreseeable risk of harm through the misconduct previously described;

c. By failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiffs' and Class members' PII both before and after learning of the Data Breach;

d. By failing to comply with the minimum industry data security standards during the period of the Data Breach; and

e. By failing to timely and accurately disclose that Plaintiffs' and Class members' PII had been improperly acquired or accessed.

115. Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect PII of Plaintiffs and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiffs and Class members during the time it was within Equifax's possession or control.

116. The law further imposes an affirmative duty on Equifax to timely disclose the

unauthorized access and theft of the PII to Plaintiffs and the Class so that Plaintiffs and Class members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

117. Equifax breached its duty to notify Plaintiffs and Class members of the unauthorized access by waiting many months after learning of the breach to notify Plaintiffs and Class members and then by failing to provide Plaintiffs and Class members information regarding the breach until September 2017. Instead, its executives disposed of at least $1.8 million worth of shares in the company after Equifax learned of the data breach but before it was publicly announced. To date, Equifax has not provided sufficient information to Plaintiffs and Class members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and the Class.

118. Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect PII of Plaintiffs and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiffs and Class members during the time it was within Equifax's possession or control.

119. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Equifax prevented Plaintiffs and Class members from taking meaningful, proactive steps to secure their financial data and bank accounts.

120. Upon information and belief, Equifax improperly and inadequately safeguarded PII of Plaintiffs and Class members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Equifax's failure to take proper security measures to protect sensitive PII of Plaintiffs and Class members as described in this Complaint,

created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of PII of Plaintiffs and Class members.

121. Equifax's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to PII of Plaintiffs and Class members; and failing to provide Plaintiffs and Class members with timely and sufficient notice that their sensitive PII had been compromised.

122. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

123. Equifax's Data Breach proximately caused Plaintiffs and Nationwide Class members to be exposed to fraud and to be harmed. The injuries suffered by the Plaintiffs and members of the Nationwide Class are a direct result of Equifax's breach of its duties and include: theft of their PII and financial information; costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and potential consequences of the Data Breach, including closely reviewing and monitoring their credit reports and accounts for unauthorized activity, finding fraudulent charges, cancelling and reissuing cards, closing or modifying financial accounts, purchasing credit monitoring and identity theft protection services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, which may take months if not years to discover and

detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy; the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII and financial information being placed in the hands of hackers; damages to and diminution in value of their PII and financial information entrusted to Equifax for the sole purpose of Equifax's credit-reporting services and with the mutual understanding that Equifax would safeguard Plaintiffs' and Nationwide Class members' data against theft and not allow access and misuse of their data by others; money paid to Equifax for their services during the period of the Data Breach in that Plaintiffs and members of the Nationwide Class would not have obtained, or permitted others to obtain, Equifax's credit-reporting services had Equifax disclosed that it lacked adequate systems and procedures to reasonably safeguard consumers' PII and financial information and had Equifax provided timely and accurate notice of the Data Breach; payments made to Equifax for credit reporting services in that a portion of the price paid by Plaintiffs and the Nationwide Class, or others on their behalf, to Equifax was for the costs of Equifax providing reasonable and adequate safeguards and security measures to protect customers' PII and financial data and, as a result, Plaintiffs and members of the Nationwide Class did not receive what was bargained and paid for; and continued risk to Plaintiffs and members of the Nationwide Class that their PII and financial information, which remains in the possession of Equifax and which is subject to further breaches so long as Equifax fails to undertake appropriate and adequate measures to protect it; damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiffs and Class members; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial

institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT IV
NEGLIGENCE PER SE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)

124. Plaintiffs restate and reallege Paragraphs 1 through 75 and 102 through 123 as if fully set forth herein.

125. This is a claim for relief based on common law negligence per se.

126. 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 PII. The FTC publications and orders described above also form part of the basis of Equifax's duty in this regard.

127. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Equifax's conduct was particularly unreasonable given the nature and amount of PII 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.

128. Equifax's violation of Section 5 of the FTC Act constitutes negligence per se.

129. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

130. The harm that occurred as a result of the Equifax Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class members.

COUNT V
VIOLATION OF STATE DATA BREACH STATUTES
(ON BEHALF OF PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)

131. Plaintiffs restate and reallege Paragraphs 1 through 75 as if fully set forth herein.

132. This is a claim for relief based on violations of various states' data breach statutes as enumerated below.

133. Legislatures in the states and jurisdictions listed below have enacted data breach statutes. These statutes generally require that any person or business conducting business within the state that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system to any resident of the state whose personal information was acquired by an unauthorized person, and further require that the disclosure of the breach be made in the most expedient time possible and without unreasonable delay.

134. The Equifax data breach constitutes a breach of the security system of Equifax within the meaning of the below states' data breach statutes and the data breached is protected and covered by the below data breach statutes.

135. Plaintiffs' and Class members' names, social security numbers, phone numbers, driver's license numbers, birth dates, credit card numbers and email addresses constitute personal

information under and subject to the below state data breach statutes.

136. Equifax unreasonably delayed in informing the public, including Plaintiffs and members of the Class about the breach of security of Plaintiffs' and Class members' confidential and non-public personal information after Equifax knew or should have known that the data breach had occurred.

137. Equifax failed to disclose to Plaintiffs and Class members without unreasonable delay and in the most expedient time possible, the breach of security of Plaintiffs' and Class members' personal and financial information when Equifax knew or reasonably believed such information had been compromised.

138. Plaintiffs and members of the Class suffered harm directly resulting from Equifax's failure to provide and the delay in providing Plaintiffs and Class members with timely and accurate notice as required by the below state data breach statutes. Plaintiffs suffered the damages alleged above as a direct result of Equifax's delay in providing timely and accurate notice of the data breach.

139. Had Equifax provided timely and accurate notice of the Equifax data breach, Plaintiffs and Class members would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Equifax in providing notice. Plaintiffs and Class members could have contacted their banks to cancel their cards, or could otherwise have tried to avoid the harm caused by Equifax's delay in providing timely and accurate notice.

140. Equifax's failure to provide timely and accurate notice of the Equifax data breach violated the following state data breach statutes:

a. Alaska Stat. Ann. § 45.48.010(a), et seq.;

b. Ark. Code Ann. § 4-110-105(a), et seq.;

c. Cal. Civ. Code § 1798.83(a), et seq.;

d. Colo. Rev. Stat. Ann § 6-1-716(2), et seq.;

e. Conn. Gen. Stat. Ann. § 36a-701b(b), et seq.;

f. Del. Code Ann. Tit. 6 § 12B-102(a), et seq.;

g. D.C. Code § 28-3852(a), et seq.;

h. Fla. Stat. Ann. § 501.171(4), et seq.;

i. Ga. Code Ann. § 10-1-912(a), et seq.;

j. Haw. Rev. Stat. § 487N-2(a), et seq.;

k. Idaho Code Ann. § 28-51-105(1), et seq.;

l. Ill. Comp. Stat. Ann. 530/10(a), et seq.;

m. Iowa Code Ann. § 715C.2(1), et seq.;

n. Kan. Stat. Ann. § 50-7a02(a), et seq.;

o. Ky. Rev. Stat. Ann. § 365.732(2), et seq.;

p. La. Rev. Stat. Ann. § 51:3074(A), et seq.;

q. Md. Code Ann., Commercial Law § 14-3504(b), et seq.;

r. Mass. Gen. Laws Ann. Ch. 93H § 3(a), et seq.;

s. Mich. Comp. Laws Ann. § 445.72(1), et seq.;

t. Minn. Stat. Ann. § 325E.61(1)(a), et seq.;

u. Mont. Code Ann. § 30-14-1704(1), et seq.;

v. Neb. Rev. Stat. Ann. § 87-803(1), et seq.;

w. Nev. Rev. Stat. Ann. § 603A.220(1), et seq.;

x. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), et seq.;

y. N.J. Stat. Ann. § 56:8-163(a), et seq.;

z. N.C. Gen. Stat. Ann. § 75-65(a), et seq.;

aa. N.D. Cent. Code Ann. § 51-30-02, et seq.;

bb. Okla. Stat. Ann. Tit. 24 § 163(A), et seq.;

cc. Or. Rev. Stat. Ann. § 646A.604(1), et seq.;

dd. R.I. Gen. Laws Ann. § 11-49.2-3(a), et seq.;

ee. S.C. Code Ann. § 39-1-90(A), et seq.;

ff. Tenn. Code Ann. § 47-18-2107(b), et seq.;

gg. Tex. Bus. & Com. Code Ann. § 521.053(b), et seq.;

hh. Utah Code Ann. § 13-44-202(1), et seq.;

ii. Va. Code. Ann. § 18.2-186.6(B), et seq.;

jj. Wash. Rev. Code Ann. § 19.255.010(1), et seq.;

kk. Wis. Stat. Ann. § 134.98(2), et seq.; and

ll. Wyo. Stat. Ann. § 40-12-502(a), et seq.

141. Plaintiffs and members of each of the statewide Data Breach Statute Classes seek all remedies available under their respective state data breach statutes, including but not limited to a) damages suffered by Plaintiffs and Class members as alleged above, b) equitable relief, including injunctive relief, and c) reasonable attorney fees and costs, as provided by law.

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

142. Plaintiffs reallege and incorporate paragraphs 1 through 75 above.

143. This is a statutory claim for relief based on Equifax's violations of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201, et seq. ("FDUTPA")

144. Equifax's business practices alleged herein constitute unfair and/or deceptive methods, acts, or practices under FDUTPA.

145. At all relevant times, Plaintiffs and Florida Subclass members were "consumers" within the meaning of the FDUTPA, Fla. Stat. § 501.203(7).

146. Equifax's conduct occurred in the conduct of "trade and commerce" within the meaning of the FDUTPA, Fla. Stat. § 501.203(8).

147. Equifax's practices violated the FDUTPA by engaging in unconscionable, deceptive, unfair acts or practices, including, but not limited to:

a. Failing to maintain adequate and reasonable data security standards to safeguard for the Plaintiffs' and Florida Subclass members' PII and financial information from unauthorized disclosure, release, data breaches, and theft, in violation of state and federal laws and its own privacy practices and policies;

b. Knowingly and fraudulently misrepresenting that it would maintain adequate and reasonable data security standards for Plaintiffs' and the Florida Subclass members' PII and financial information from unauthorized disclosure, release, data breaches, and theft;

c. Knowingly omitting, suppressing, and concealing the inadequacy of its data security protections for the Plaintiffs' and Florida Subclass members' PII and financial information; and

d. Failing to disclose the Data Breach to Plaintiffs and the members of the Florida Subclass in a timely and accurate manner.

148. Equifax knew or should have known that its computer systems and data security practices and measures failed to meet legal and industry standards, were inadequate to safeguard the Plaintiffs' and Florida Subclass members' PII and financial information, and that the risk of a data breach or theft was highly likely given the lack of employing adequate security measures.

149. Equifax's actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and members of the Florida Subclass. Equifax's failure to disclose such material information rendered its representations of its data security

practices as likely to deceive a reasonable consumer.

150. Equifax knew such facts would (a) be unknown to and not easily discoverable by Plaintiffs and members of the Florida Subclass; and (b) defeat Plaintiffs' and the Florida Subclass members' ordinary, foreseeable and reasonable expectations concerning the security of Equifax's data systems.

151. An objective, reasonable person would have been deceived by Equifax's representations about the security and protection of data in its databases and networks.

152. Equifax's course of trade or commerce, were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Equifax that applied to Plaintiffs and the Florida Subclass and were repeated continuously before and after Equifax obtained confidential PII and financial information concerning Plaintiffs and Florida Subclass members, all of whom have been adversely affected and harmed by Equifax's conduct and the public was and is at risk as a result thereof.

153. Equifax's acts, omissions, and practices proximately caused Plaintiffs and Florida Subclass members to suffer damages including incurring costs associated with protecting PII and financial information that has been exposed; costs associated with the theft of their identities, such as time and expenses associated with credit monitoring, decrease in credit ratings, financial harm suffered as a result of accounts opened and used without their knowledge or authorization, and time and expense associated with closing accounts opened and used without their knowledge or authorization. Plaintiffs and Florida Subclass members also suffered damages in that they did not obtain the value of the goods and services for which they paid; were induced to pay for (or pay more for) services that they otherwise would not have; and they lost their ability to make informed and reasoned decisions about Equifax's services.

154. As a direct and proximate result of Equifax's violations of FDUTPA, Plaintiffs and Florida Subclass members also suffered injuries to legally protected interests, as described above, including but not limited to their legally protected interest in the confidentiality and privacy of their PII and financial information, including confidential records, time and expenses related to monitoring their financial accounts for fraudulent activity, and increased, imminent risk of fraud and identity theft, and loss of value of their personal identification and financial information.

155. As a direct and proximate cause of these practices, Plaintiffs and Florida Subclass members suffered an ascertainable loss.

156. The above unfair and deceptive trade practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury and damage to Plaintiffs and Florida Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition. These acts were within common law, statutory, or other established concepts of fairness.

157. As a direct and proximate result of Equifax's unlawful, unfair, and fraudulent business practices, Plaintiffs and members of the Florida Subclass have suffered injury in fact and are entitled to relief, including restitution, declaratory relief, and a permanent injunction enjoining Equifax from its unlawful and unfair practices.

158. Plaintiffs and the Florida Subclass seek actual damages under Fla. Stat. § 501.211(2) and all fees, costs, and expenses allowed by law, including attorney's fees and costs, pursuant to Federal Rule of Civil Procedure 23 and Fla. Stat. §§ 501.2105 and 501.211, in an amount to be proven at trial.

159. Plaintiffs and the Florida Subclass also seek injunctive and declaratory relief,

including an order that Equifax immediately cease and desist its unfair and deceptive acts and practices, under Florida Statutes § 501.211.

160. Equifax's conduct caused and continues to cause substantial injury to Plaintiffs and Florida Subclass members. Equifax will continue to maintain Plaintiffs' and Florida Subclass members' PII and financial information for the indefinite future. Unless injunctive relief is granted, Plaintiffs and Florida Subclass members, who do not have an adequate remedy at law, will continue to suffer harm, and the balance of equities favors Plaintiffs and Florida Subclass members.

161. Plaintiffs and Florida Subclass members seek declaratory and injunctive relief as permitted by law or equity to assure that the Plaintiffs and the Florida Subclass have an effective remedy, including enjoining Equifax from continuing the unlawful practices as set forth above, along with any other relief the Court deems just and proper under FDUTPA.

COUNT VII
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE SEPARATE STATEWIDE CLASSES)

162. Plaintiffs restate and reallege Paragraphs 1 through 75 as if fully set forth herein.

163. As previously alleged, Plaintiffs and Class members entered into an implied contract that required Equifax to provide adequate security for the PII it collected from their payment card transactions. As previously alleged, Equifax owes duties of care to Plaintiffs and Class members that require it to adequately secure PII.

164. Equifax still possesses PII pertaining to Plaintiffs and Class members.

165. Equifax has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems.

166. Accordingly, Equifax has not satisfied its contractual obligations and legal duties

to Plaintiffs and Class members. In fact, now that Equifax's lax approach towards data security has become public, the PII in its possession is more vulnerable than previously.

167. Actual harm has arisen in the wake of the Equifax Data Breach regarding Equifax's contractual obligations and duties of care to provide data security measures to Plaintiffs and Class members.

168. Plaintiffs, therefore, seek a declaration that (a) Equifax's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Equifax must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. Purging, deleting, and destroying in a reasonable secure manner PII not necessary for its provisions of services;

f. Conducting regular database scanning and securing checks;

g. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against EQUIFAX as follows:

a. For an Order certifying the Classes, as defined herein, and appointing Plaintiffs and their Counsel to represent the Nationwide Class, or in the alternative the separate Statewide Classes or Florida Subclass;

b. For an Order finding that Equifax breached its duty to safeguard and protect the PII and financial information of Plaintiffs and members of the Classes that was compromised in the Data Breach;

c. For an award of damages, as allowed by law in an amount to be determined;

d. For equitable relief enjoining Equifax from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and Class members;

e. For equitable relief compelling Equifax to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to Class members the type of PII compromised;

f. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

g. For pre-judgment and postjudgment interest as prescribed by law; and

h. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable as a matter of right.

Dated: September 25, 2017

Thomas V. Girardi
California Bar No. 36603
Christopher T. Aumais
California Bar No. 249901
GIRARDI | KEESE
Pro Hac Vice Motions to be Filed
1126 Wilshire Boulevard
Los Angeles, California 90017
Telephone: (213) 977-0211
Facsimile: (213) 481-1554
Email: tgirardi@girardikeese.com
Email: caumais@girardikeese.com

RUSSOMANNO & BORRELLO, P.A.
Museum Tower – Penthouse 2800
150 West Flagler Street
Miami, Florida 33130
Telephone: (305) 373-2101
Facsimile: (305) 373-2103

By:/s/ Herman J. Russomanno
Herman J. Russomanno (Fla. Bar No. 240346)
hrussomanno@russomanno.com
Robert J. Borrello (Fla Bar No 764485)
rborrello@russomanno.com
Herman J. Russomanno (Fla. Bar No. 21249)
herman2@russomanno.com

Edward G. Rubinoff
Florida Bar No. 97785
Andrew Moss
Florida Bar No. 0170259
KUTNER, RUBINOFF & MOSS
2665 S. Bayshore Drive, Ste. 30 I
Coconut Grove, FL 33133
Tel: 305-358-6200
Fax: 305-577-8230
Email: rubinoff@krmlegal.com
Email: moss@krmlegal.com

David A. Nunez
Florida Bar No. 646776
MEYER & NUNEZ, P.A.
150 W. Flagler Street, Ste. 2700
Miami, FL 33130
Tel: 305-722-9898
Fax: 305-3 71-9197
Email: david@nunez-law.com

Attorneys for Plaintiffs and the Classes

JS 44 (Rev. 06/17) FLSD Revised 06/01/2017

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS Jacqueline Martinez and Barron A. Libasci, on behalf of themselves and all similarly situated

DEFENDANTS EQUIFAX, INC.,

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

County of Residence of First Listed Defendant Fulton County, Georgia
(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, and Telephone Number)*

Russomanno & Borrello, P.A., Museum Tower - Penthouse 2800
150 W. Flagler Street, Miami, Florida 33130; 305-373-2101

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)*

Click here for: Nature of Suit Code Descriptions

CONTRACT
☐ 110 Insurance
☐ 120 Marine
☐ 130 Miller Act
☐ 140 Negotiable Instrument
☐ 150 Recovery of Overpayment & Enforcement of Judgment
☐ 151 Medicare Act
☐ 152 Recovery of Defaulted Student Loans (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
☐ 362 Personal Injury - Med. Malpractice

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

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

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

PRISONER PETITIONS
Habeas Corpus:
☐ 463 Alien Detainee
☐ 510 Motions to Vacate Sentence
Other:
☐ 530 General
☐ 535 Death Penalty
☐ 540 Mandamus & Other
☐ 550 Civil Rights
☐ 555 Prison Condition
☐ 560 Civil Detainee – Conditions of Confinement

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

LABOR
☐ 710 Fair Labor Standards Act
☐ 720 Labor/Mgmt. Relations
☐ 740 Railway Labor Act
☐ 751 Family and Medical Leave Act
☐ 790 Other Labor Litigation
☐ 791 Empl. Ret. Inc. Security Act

IMMIGRATION
☐ 462 Naturalization Application
☐ 465 Other Immigration Actions

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

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

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

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

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

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

☑ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Re-filed **(See VI below)** ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district *(specify)* ☐ 6 Multidistrict Litigation Transfer ☐ 7 Appeal to District Judge from Magistrate Judgment ☐ 8 Multidistrict Litigation – Direct File ☐ 9 Remanded from Appellate Court

VI. RELATED/ RE-FILED CASE(S)

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

JUDGE:

DOCKET NUMBER: See attached 4 cases

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)***:
15 USC 1681 - Class Action as to Defendant's Data Breach of Confidential Information

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

DATE 9/25/17

SIGNATURE OF ATTORNEY OF RECORD [signature] Flo Bar No. 21249

FOR OFFICE USE ONLY

RECEIPT # AMOUNT IFP JUDGE MAG JUDGE

Related Pending Cases in the S.D. Fla.

1. 17-23405-CIV
2. 17-23465-CIV
3. 17-61833-CIV
4. 17-81056-CIV

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

UNITED STATES DISTRICT COURT

for the

Southern District of Florida

JACQUELINE MARTINEZ, and BARRON A. LIBASCI, on behalf of themselves and all others similarly situated,

Plaintiff(s)

v.

EQUIFAX, INC.,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)*

EQUIFAX, INC.
c/o The Prentice Hall Corporation System, Inc.
1201 Hays Street, Suite 105
Talllahassee, Florida 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:

Herman J. Russomanno III, Esq.
Russomanno & Borrello, P.A.
Museum Tower - Penthouse 2800
150 W. Flagler Street
Miami, Florida 33130
herman2@russomanno.com

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:

Print Save As... Reset