UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

GREGG PODALSKY and EILEEN SUE SAMILOW, Individually and on Behalf of All Others Similarly Situated, Plaintiffs, vs. EQUIFAX, INC., Defendant.	Civil Action No. **CLASS ACTION** COMPLAINT FOR VIOLATIONS OF FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, NEGLIGENCE, VIOLATION OF FAIR CREDIT REPORTING ACT AND DECLARATORY RELIEF DEMAND FOR JURY TRIAL

Plaintiffs, Gregg Podalsky and Eileen Sue Samilow, individually and on behalf of all others similarly situated ("Plaintiffs"), by their undersigned attorneys, bring this class action complaint against Defendant, Equifax Inc. ("Equifax," the "Company," or "Defendant"), based on personal knowledge as to themselves and upon information and belief as to all other matters based on the investigation of counsel.

I. NATURE OF ACTION

1. Equifax is one of the three largest consumer credit reporting agencies in the United States, collecting data on more than 820 million consumers and more than 91 million businesses worldwide.

2. As part of its business, Equifax collects and stores personal information about consumers, including, for example, names, social security numbers, birthdates, addresses and driver's license numbers.

3. Equifax proclaims itself to be "a leader in managing and protecting data,"[1] and assures consumers that it is "committed to protecting the security of [their] personal information and use[s] technical, administrative and physical security measures that comply with applicable federal and state laws."[2]

4. Equifax has failed to live up to those promises.

5. Equifax has allowed repeated security breaches in recent years, and the Company failed to improve its security practices despite the glaring red flags of those previous thefts, paving the way for one of the most severe cyber-attacks in recent years.

6. Most recently on September 7, 2017, Equifax announced a "cybersecurity incident" involving "criminals exploit[ing] a U.S. website application vulnerability to gain access to certain files."

7. The breach is estimated to impact at least ***143 million U.S. consumers***.

8. The stolen data includes the personal information the Company collects and uses for its own profit – consumers' names, social security numbers, birthdates, addresses and driver's license numbers. As part of the breach, "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 compromised in the security failure.[3]

9. Reports say that while this data breach was not the largest in sheer size, it is ***worse in terms of severity*** as "[t]hieves were able to siphon far more personal information – the keys that

---

[1] *Equifax Announces Cybersecurity Incident Involving Consumer Information*, PRNewswire, Sept. 7, 2017, http://www.prnewswire.com/news-releases/equifax-announces-cybersecurity-incident-involving-consumer-information-300515960.html (last visited Sept. 12, 2017).

[2] Equifax Privacy, Equifax Personal Products, Apr. 24, 2017, http://www.equifax.com/privacy/equifax-personal-products (last visited Sept. 12, 2017).

[3] *Id*. (all emphasis is added unless otherwise stated).

unlock consumers' medical histories, bank accounts and employee accounts."[4]

10. As a result of Defendant's failure to establish and implement basic data security protocols, consumers' personal information is now in the hands of criminals and/or enemies of the Unites States, subjecting Plaintiff and the Class (as defined below) to the serious risk of identity theft in a wide variety of forms.

11. The scope of the breach is massive. An executive director of the nonprofit research group the World Privacy Forum opined, "'***[i]f you have a credit report, chances are you may be in this breach. The chances are much better than 50 percent.***'"[5]

12. In contrast to other security breaches, e.g., Target and Home Depot, many people affected by the breach may not even be aware that Equifax collects, maintains and distributes, for profit, their personal identifying information. Unlike a typical customer-company relationship, Equifax commonly gains access to, and then collects and stores data from various entities, including credit card companies, banks, retailers and lenders that transfer credit activity of their own customers to the major consumer credit reporting agencies like Equifax, or by purchasing public records.

13. The breach took place from mid-May through July 2017. Equifax reportedly discovered the breach on July 29, 2017. Equifax waited ***six weeks***, however, to disclose the breach to consumers. The *Los Angeles Times* reported, "[t]hat's six weeks that consumers could have been victimized without their knowledge and therefore left without the ability to take countermeasures.

[4] Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber, *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, The New York Times, Sept. 7, 2017, https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?mcubz=3 (last visited Sept. 12, 2017).
[5] *Id.*

Equifax has not explained the delay."[6]

14. Shortly after the discovery of the breach, but prior to its public disclosure, three Equifax executives sold nearly 2 million dollars' worth of Equifax stock. The sales came just three and four days after Equifax discovered the breach, and included Equifax's Chief Financial Officer selling almost a million dollars' worth of stock, and its President of U.S. Information Services selling over a half-a-million dollars' worth of stock. In the first full day of trading after the breach announcement, Equifax's share price closed down approximately 13%.

15. On or around September 7, 2017, Equifax set up a system that could put the victims of its own security breach at further risk. As part of Equifax's announcement of the breach, it set up a website to purportedly "help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection," calling the offering "TrustedID Premier."[7] But, according to at least one report:

> The firm set up a website allowing individuals to check if their information was potentially compromised, but it requires users to plug in their last name and last six digits of their Social Security numbers. ***That raises the question of why anyone would trust Equifax with even a partial Social Security number at this stage***.[8]

To the extent potentially affected consumers sought to bypass the Equifax website in order to check to see if their information was compromised, one reporter found on the day after the

[6] Michael Hiltzik, *Here are all the ways the Equifax data breach is worse than you can imagine*, L.A. Times, Sept. 8, 2017, http://www.latimes.com/business/hiltzik/la-fi-hiltzik-equifax-breach-20170908-story.html (last visited Sept. 12, 2017).
[7] *Equifax Announces Cybersecurity Incident Involving Consumer Information*, PRNewswire, Sept. 7, 2017, http://www.prnewswire.com/news-releases/equifax-announces-cybersecurity-incident-involving-consumer-information-300515960.html (last visited Sept. 12, 2017).
[8] Michael Hiltzik, *Here are all the ways the Equifax data breach is worse than you can imagine*, L.A. Times, Sept. 8, 2017, http://www.latimes.com/business/hiltzik/la-fi-hiltzik-equifax-breach-20170908-story.html (last visited Sept. 12, 2017).

announcement that the phone number provided was busy the entire time he wrote his article.[9]

16. In order to sign up for the "free" credit file monitoring and identity theft products, as of September 8, 2017, Equifax required customers potentially affected by the breach to agree to terms and conditions that included an arbitration provision and a class action waiver.[10] Days later, the Company acquiesced to pressure to remove that provision. But, the credit monitoring service is only offered for free for one year, even though hackers can exploit stolen personal data for years to come, and "it gives Equifax a lucrative database of possible customers to be sold continuing subscriptions for the service after the year is expired – at a price currently set at $19.95 a month."[11] Typically, enrollment in this type of service requires consumers to provide a credit card number, which is then used to automatically bill them after the end of the free trial.[12]

17. Plaintiffs' personal information was compromised as a result of Equifax's negligent, reckless, willful or intentional acts and omissions in failing to take reasonable measures to ensure that its security systems would adequately protect consumers' personal identifying information, failing to disclose to consumers that it did not have adequate security systems in place to protect and safeguard consumers' information, and failing to disclose the breach in a timely fashion. Indeed, one fraud prevention company "***saw a 'significant' spike" in account takeover attempts – a 15% increase year-over-year – in the last two months***, suggesting the increased

---

[9] Jake Swearingen, *Equifax Screwed Up Its Data Breach From Nearly Every Angle*, New York, Sept. 8, 2017, http://nymag.com/selectall/2017/09/equifax-screwed-up-its-data-breach-from-nearly-every-angle.html (last visited Sept. 12, 2017).

[10] Wayback Machine, Equifax, *Cybersecurity Incident & Important Consumer Information – FAQs for Consumers*, Sept. 9. 2017, https://web.archive.org/web/20170909005053/https://www.equifaxsecurity2017.com/frequently-asked-questions/ (last visited Sept. 12, 2017).

[11] Michael Hiltzik, *Here are all the ways the Equifax data breach is worse than you can imagine*, L.A. Times, Sept. 8, 2017, http://www.latimes.com/business/hiltzik/la-fi-hiltzik-equifax-breach-20170908-story.html (last visited Sept. 12, 2017).

[12] *See id.*

activity could be related to the Equifax breach.[13]

18. On September 8, 2017, it was reported that New York's attorney general opened an investigation into the Equifax data breach. Attorney General Eric T. Schneiderman wrote a letter to the Company requesting specific details about the breach, and asking it to "remove language posted online that could be interpreted to mean victims of the breach could not sue or participate in a class action."[14] Congressman Ted W. Lieu of California also sent a letter to the House Judiciary Committee seeking a hearing to address the breach. Other investigations are likely.

19. Plaintiffs bring this class action lawsuit against Equifax for failing to adequately safeguard their personal information and the personal information of others. Plaintiffs seek judgment requiring Equifax to remedy the harm caused by its misconduct, which includes compensating Plaintiffs and Class members for resulting injuries sustained and for all reasonably necessary measures Plaintiffs and Class members have had to take in order to identify and safeguard the accounts put at risk by Equifax's negligent, reckless, willful or intentional acts and omissions. Plaintiffs further seek a declaratory judgment declaring, inter alia, that any limitation on liability, arbitration or class action waiver provisions in the Equifax or TrustedID Terms of Service or privacy policies that Equifax may seek to enforce to Plaintiffs' and Class members' claims against Equifax related to the data breach must be deemed unenforceable.

II. PARTIES

20. Plaintiff Gregg Podalsky is a natural person and a resident and citizen of Florida.

---

[13] Nicole Sinclair, *Expert: Fraudsters may already be trying to use breached Equifax data, Yahoo! Finance*, Sept. 12, 2017, https://finance.yahoo.com/news/expert-fraudsters-may-already-trying-use-breached-equifax-data-172337733.html (last visited Sept. 13, 2017).

[14] Tiffany Hsu, *New York's Attorney General Opens Inquiry Into Equifax Breach*, The New York Times, Sept. 8, 2017, https://www.nytimes.com/2017/09/08/business/equifax.html (last visited Sept. 8, 2017).

Mr. Podalsky is one of the more than 143 million Equifax customers whose personal information was stolen because Equifax was reckless in failing to secure such information as a result of the data breach announced by Equifax on September 7, 2017.

21. Plaintiff Eileen Sue Samilow is a natural person and a resident and citizen of Florida. Ms. Samilow is also one of the more than 143 million Equifax customers whose personal information was stolen because Equifax was reckless in failing to secure such information as a result of the data breach announced by Equifax on September 7, 2017.

22. Defendant Equifax is a Georgia corporation headquartered at 1550 Peachtree Street, N.W., Atlanta, Georgia 30309. Equifax does business throughout the State of Florida and the United States. Equifax collects data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers. The Company's common stock is traded on the New York Stock Exchange under the symbol EFX. Equifax generated $3.14 billion in operating revenue in 2016.

III. JURISDICTION AND VENUE

23. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d) ("CAFA"), because: (i) the proposed Class consists of well over 100 members; (ii) Plaintiffs are citizens of the State of Florida while Defendant is a citizen of a different state; and (iii) the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs. The Court also has jurisdiction under 28 U.S.C. §1331, and has supplemental jurisdiction over state law claims pursuant to 28 U.S.C. §1367.

24. Venue is proper in this District pursuant to 28 U.S.C. §1391 because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this judicial District. Equifax conducts business throughout Florida and regularly conducts business in this District. In

addition, the causes of action arose, in substantial part, in this District.

IV. FACTUAL ALLEGATIONS

A. Equifax Collects Vast Amounts of Sensitive Personal Information from Consumers for Financial Gain

25. Equifax is one of the three largest American credit agencies along with Experian and TransUnion. The Company was first incorporated in 1913, and its predecessor company, Retail Credit Company ("RCC"), dates back to 1899.

26. By the 1960s, RCC was one of the nation's largest credit bureaus, holding files on millions of Americans. By the end of that decade, critics of the Company's business model, including Columbia University Professor Alan Westin, attacked Equifax "for its cavalier attitude toward the accuracy of its information on consumers, and for giving out that information to practically anyone who asked for it."[15] These consumer files collected information about virtually every aspect of consumers' lives, including marital troubles, jobs, school history, childhood, sex life and political activities.

27. These practices led to the enactment of the Fair Credit Reporting Act, which provided consumers rights regarding information stored about them by companies, and in turn allegedly led to RCC changing its name to Equifax in 1975 to improve its image. By the 1990s, Equifax was the world's largest consumer-reporting organization.

28. Today, Equifax's core business is built on the backs of consumers' and businesses' personal identifying information. Specifically, the Company's "products and services are based on comprehensive databases of consumer and business information derived from numerous sources including credit, financial assets, telecommunications and utility payments, employment, income,

[15] Wired, *Separating Equifax From Fiction*, September 1, 1995, https://www.wired.com/1995/09/equifax/ (last visited Sept. 13, 2017).

demographic and marketing data."[16] Moreover, Equifax boasts that as part of its business, it "help[s] consumers understand, manage and ***protect their personal information*** . . . ."[17]

29. Equifax collects substantial amounts of personal information about consumers, whether those consumers have a direct relationship with the Company or not. By the Company's own recent admissions, at a minimum, Equifax collects, maintains, analyzes and sells a plethora of sensitive consumer information, including consumers' names, social security numbers, birthdates, addresses, driver's license numbers, credit card numbers and dispute documents containing further personal identifying information. All of this information was admittedly compromised by the recent security breach.

30. Equifax defines "personally identifiable information" in its online Privacy Policy as information the Company collects "from *you as an individual* online to verify your identity and to process your requests as an individual," and includes, in addition to the categories of information referred to above, gender, home telephone numbers, e-mail addresses, current and former mailing addresses and credit card expiration dates.[18]

B. Equifax Assures Consumers that It Safeguards Their Personal Information

31. Equifax maintains separate privacy policies for consumers who utilize Equifax "personal products for individual or household purposes" ("Products Policy") and for consumers who "use the US Equifax.com web site to obtain a free or reduced-fee disclosure of your credit file, dispute item(s) on [their] credit file, request that an initial fraud alert or an active duty alert be

[16] Equifax Form 10-K for the fiscal year ending December 31, 2016, https://otp.tools.investis.com/clients/us/equifax/SEC/sec-show.aspx?Type=html&FilingId=11875154&CIK=0000033185&Index=10000.
[17] *Id.*
[18] Equifax, *Privacy Policy*, http://www.equifax.com/privacy_policy/ (last visited Sept. 10, 2017) (emphasis in original).

placed on [their] credit file, or take any action associated with a security freeze on [their] credit file" ("Credit Policy").[19] Separately, Equifax maintains a privacy policy applicable to "Equifax's commitment to privacy in an online setting" that governs nine different U.S. Equifax websites ("Online Policy").[20]

32. Equifax's Products Policy describes the efforts the Company makes to safeguard consumers' personal information as follows: "We are committed to protecting the security of your personal information and use technical, administrative and physical security measures that comply with applicable federal and state laws."[21]

33. Equifax's Credit Policy describes the efforts the Company makes to safeguard consumers' personal information as follows: "[w]e are committed to protecting the security of your information through procedures and technology designed for this purpose by taking these steps: Before we provide you access to your credit file disclosure, we verify your identity."[22] The Credit Policy also provides the following additional assurances.

- We limit access to your personal information to employees having a reasonable need to access this information to provide products and services to you. Employees who misuse information are subject to disciplinary action, including termination.

- We have reasonable physical, technical and procedural safeguards to help protect your personal information.

- In areas that contain your personal information, we use secure socket layer (SSL) encryption to help protect this information while it is in transit between

[19] *Cf.* Equifax, *Equifax Personal Products*, http://www.equifax.com/privacy/equifax-personal-products (last visited Sept. 11, 2017) *with* Equifax, *Personal Credit Reports*, http://www.equifax.com/privacy/personal-credit-reports (last visited Sept. 11, 2017).
[20] Equifax, *Privacy Policy*, http://www.equifax.com/privacy_policy/ (last visited Sept. 10, 2017).
[21] Equifax, *Equifax Personal Products*, http://www.equifax.com/privacy/equifax-personal-products (last visited Sept. 11, 2017).
[22] Equifax, *Personal Credit Reports*, http://www.equifax.com/privacy/personal-credit-reports (last visited Sept. 11, 2017).

our servers and your computer.[23]

34. Equifax's Online Policy describes that the Company built its "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 . . . . ***Safeguarding the privacy and security of information, both online and offline is a top priority for Equifax***."[24] The Online Policy further describes in detail Equifax's purported security and confidentiality guidelines and/or procedures.

> Equifax recognizes the importance of secure online transactions, and we maintain physical, administrative, and technical safeguards to protect your personally identifiable information, your business organization identifiable information, and the other information we collect about you, as described above.
>
> We safeguard the privacy of information you provide us through online forms. For online requests and Personal Solutions product orders and service requests, we use programs that encrypt the information you provide on the form before transmission to Equifax. Information you provide to us online, including personally identifiable information and business organization identifiable information, is transmitted to us through a secured socket layer (SSL) transmission. The information is decrypted only upon receipt by Equifax.
>
> Except as stated in the "To Whom We Disclose The Information We Collect" section above, we restrict access to *personally identifiable information and business organization identifiable information* that is collected about you to only those who have a need to know that information in connection with the purposes for which it is collected and used.
>
> Additionally, we have security protocols and measures in place to protect the *personally identifiable information*, business organization identifiable information and other information we maintain about you from unauthorized access or alteration. These measures include internal and external firewalls, physical security and technological security measures, and encryption of certain data. When *personally identifiable information* is disposed of, it is disposed of in a secure manner.

[23] *Id.*

[24] Equifax, *Privacy Policy*, http://www.equifax.com/privacy_policy/ (last visited Sept. 10, 2017).

> You also have a role in protecting the security of information about you. For example, you should guard your password to the Personal Solutions Member Center and not permit unauthorized use of your account for Personal Solutions products. Additionally, you should close your browser when have finished viewing your information on the Equifax web site to protect the privacy of your individual or business organization information.[25]

35. Equifax's Chief Executive Officer, Richard F. Smith, reassured consumers in the Company's press release announcing the data breach saying that "[w]e pride ourselves on being a leader in managing and protecting data."[26]

C. Equifax's History of Lax Security Systems and Resulting Data Breaches

36. Equifax has endured a pattern of security systems breaches in recent years. For example, in 2014, Equifax wrote to the New Hampshire attorney general about a security breach that affected New Hampshire residents involving an "IP address operator [that] was able to obtain [] credit reports using sufficient personal information to meet Equifax's identity verification process."[27] From April 2013 to January 31, 2014 Equifax reported that the IP address "may have made unauthorized inquiries to Equifax credit reports and credit reports may have been fraudulently ordered by the operator of the IP address."[28]

37. In 2016, a security researcher uncovered a common vulnerability known as cross-site scripting ("XSS") on the main Equifax website. 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

[25] *Id.* (emphasis in original).
[26] Press Release, PRNewswire, *Equifax Announces Cybersecurity Incident Involving Consumer Information* (Sept. 7, 2017), http://www.prnewswire.com/news-releases/equifax-announces-cybersecurity-incident-involving-consumer-information-300515960.html.
[27] Letter from Troy G. Krubes, Vice President and Associate Group Counsel, to Joseph Foster, Attorney General, March 5, 2014, https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20140305.pdf.
[28] *Id.*

username and password can be revealed to the hacker."[29]

38. In another instance, hackers penetrated an Equifax subsidiary's (Equifax Workforce Solutions, a/k/a TALX Corporation) W-2 Express website in May 2016, resulting in 431,000 names, addresses, social security numbers and other personal information of Kroger being leaked and triggering class action litigation. The flaw in the system in this instance was Equifax's decision to have client employees access their data using default PIN numbers. In closing the lawsuit in September 2016, the parties reported that Equifax stopped using the default PINs.

39. Problems with PINs, however, continued for Equifax well into this year. In May 2017, it was reported that hackers "were able to reset the 4-digit PIN given to customer employees as a password and then steal W-2 tax data after successfully answering personal questions about those employees."[30] Equifax stated in a boilerplate text sent to several affected customers that the unauthorized access to customers' records occurred between April 17, 2016 and March 29, 2017. The seasoned cybersecurity reporter that broke the story concluded that Equifax's TALX subsidiary actually "***aided tax thieves by relying on outdated and insufficient customer authentication methods***."[31]

40. After the public disclosure of the security breach announced September 7, 2017, and admitted website vulnerability, security researchers have been probing Equifax's infrastructure and finding concerning results. They determined that old technologies are running

[29] Thomas Fox-Brewster, *A Brief History Of Equifax Security Fails*, Forbes, Sept. 8, 2017, https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#7211fbfd677chttps://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#7211fbfd677c.

[30] Brian Krebs, *Fraudsters Exploited Lax Security at Equifax's TALX Payroll Division*, Krebs on Security, May 18, 2017, https://krebsonsecurity.com/2017/05/fraudsters-exploited-lax-security-at-equifaxs-talx-payroll-division/.

[31] *Id.*

on Equifax's website – technologies that could be ripe for further cyber-attacks. One researcher found "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," while another security professional with 17 years' experience helping protect businesses found "a weird mix of IBM Web Sphere, Apache Struts, Java . . . ***it's like stepping back in time a decade***."[32]

D. The Security Breach

41. According to Equifax, it first learned of a potentially massive data breach on July 29, 2017. Without any explanation, the Company waited almost six weeks to announce "a cybersecurity incident potentially impacting approximately ***143 million U.S. consumers***."[33] According to Equifax, "[c]riminals exploited a U.S. website application vulnerability to gain access to certain files."[34] The Company's investigation determined that the breach occurred from mid-May through July 2017.

42. While "[t]he information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers[,] . . . 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 [also] accessed."[35] Additionally, Equifax identified unauthorized access to personal information of UK and Canadian residents.

---

[32] Thomas Fox-Brewster, *A Brief History Of Equifax Security Fails*, Forbes, Sept. 8, 2017, https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#7211fbfd677chttps://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#7211fbfd677c.

[33] Press Release, PRNewswire, *Equifax Announces Cybersecurity Incident Involving Consumer Information* (Sept. 7, 2017), http://www.prnewswire.com/news-releases/equifax-announces-cybersecurity-incident-involving-consumer-information-300515960.html.

[34] *Id.*

[35] *Id.*

43. The Company says it hired an independent firm to conduct "a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted."[36] The investigation, while purportedly substantially complete, "remains ongoing and is expected to be completed in the coming weeks."[37] But, despite the early staged and open-ended nature of the inquiry and massive amounts of personal information compromised, Equifax already announced that it "has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases," potentially providing false reassurance to affected consumers.[38]

44. Articles discussing the data breach immediately pointed to the severity of the attack. One privacy executive called the incident "***about as bad as it gets***."[39] A fraud analyst at a leading research and advisory company, stated, ***"[o]n a scale of 1 to 10 in terms of risk to consumers, this is a 10***."[40] Other reports indicate that this was one of the most severe security breaches in history given the sheer scope of information obtained and potential of affecting over half of U.S. adults. As one report explained, "[i]f thieves wanted to hit one place to grab all the data needed to do the most damage, they would go straight to one of the three major credit reporting agencies."[41]

45. In connection with Equifax's September 7, 2016 press release announcing the attack, the Company directed consumers to a website, www.equifaxsecurity2017.com, to assist consumers in determining if their information has been impacted and to allow them to enroll in the TrustedID Premier program, which provides credit file monitoring and identity theft protection.

---

[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber, *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, The New York Times, Sept. 7, 2017, https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?mcubz=3.
[40] *Id.*
[41] *Id.*

46. The website, however, "requires users to plug in their last name and last six digits of their Social Security numbers. That raises the question of why anyone would trust Equifax with even a partial Social Security number at this stage."[42] And, because the TrustedID Premier enrollment period ends on November 21, 2017, consumers who wish to protect their information after that date are without any remedy.

47. In order to sign up for the "free" credit file monitoring and identity theft products, Equifax, as of September 8, 2017, required customers potentially affected by the breach to sign an arbitration provision that includes a class action waiver. Equifax later removed that language from the Terms of Use on the website, stating that it "will not apply any arbitration clause or class action waiver against consumers for claims related to the free products offered in response to the cybersecurity incident or for claims related to the cybersecurity incident itself.[43]

48. The credit monitoring service is offered for free for one year.

49. Because hackers' maintain the ability to exploit stolen personal data for several years, the service gives Equifax a lucrative database of possible customers to be sold continuing subscriptions for the service after the year is expired – at a price currently set at $19.95 a month."[44]

50. On top of the damage caused to consumers by the data breach, Equifax executives sold millions of dollars' worth of stock just days after the Company discovered the breach but several weeks before it revealed the attack to the public. Specifically, Chief Financial Officer John

[42] Michael Hiltzik, *Here are all the ways the Equifax data breach is worse than you can imagine*, L.A. Times, Sept. 8, 2017, http://www.latimes.com/business/hiltzik/la-fi-hiltzik-equifax-breach-20170908-story.html.
[43] Equifax, *Cybersecurity Incident & Important Consumer Information – FAQs for Consumers*, https://www.equifaxsecurity2017.com/frequently-asked-questions/ (last visited Sept. 10, 2017).
[44] Michael Hiltzik, Here are all the ways the Equifax data breach is worse than you can imagine, L.A. Times, Sept. 8, 2017, http://www.latimes.com/business/hiltzik/la-fi-hiltzik-equifax-breach-20170908-story.html (last visited Sept. 12, 2017).

Gamble sold $946,374 worth of stock, President of U.S. Information Solutions Joseph Loughran sold $584,099 worth of stock and Rodolfo Ploder, President of Workforce Solutions, sold $250,458 worth of stock.

E. The Equifax Data Breach Caused Plaintiffs and Class Members to Suffer Injury and Otherwise Exposed Them to Imminent Heightened Risk of Identity Theft

51. The information compromised in Equifax's data breach are highly valuable to identity thieves. In addition, social security numbers, credit and debit card information, names, email addresses, telephone numbers, dates of birth and driver's license numbers can all be used to gain access to a variety of existing accounts and websites.

52. Consumers regularly suffer a variety of consequences from data breach, including forged credit applications, the opening of unauthorized credit card accounts, fake IRS tax returns being filed under the user's name, fraudulent charges, email hacks, unauthorized access to payment accounts, stolen gift card account numbers redeemable at online merchants, and numerous other identity theft-related damages.

53. Identity thieves can also use personal identifying information to harm Plaintiffs and Class members through embarrassment, blackmail or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of

> dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[45]

54. To put it into context, the 2013 Norton Report, based on one of the largest consumer cybercrime studies ever conducted, estimated that the global price tag of cybercrime was around $113 billion at that time, with the average cost per victim being $298. That number has no doubt increased exponentially in recent years given the number of recent high-profile data breaches, and it will continue to grow in the wake of the Equifax breach.

55. The problems associated with identity theft are exacerbated by the fact that many identity thieves will wait years before attempting to use the personal information they have obtained. Indeed, a Government Accountability Office study found that "stolen data may be held for up to one year or more before being used to commit identity theft."[46] In order to protect themselves, Class members will need to remain vigilant against unauthorized data use for years and decades to come.

56. Once stolen, personal data can be used in different ways. One of the most common is that it is offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a special browser which

---

[45] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, Federal Trade Commission, April 2007, http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf.

[46] Report to Congressional Requesters, *Personal Information, Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. Government Accountability Office, June 2007, www.gao.gov/new.items/d07737.pdf.

aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and stolen personal identifying information.[47]

57. Once personal identifying information is compromised, it can then be used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be stolen from the victim's accounts, as well as from those belonging to the victim's family, friends, and colleagues.

58. Plaintiffs' and Class members' personal information was compromised as a result of Equifax's negligent, reckless, willful or intentional acts and omissions in failing to take reasonable measures to ensure that its security systems would adequately protect consumers' personal identifying information, failing to disclose to consumers that it did not have adequate security systems in place to protect and safeguard consumers' information, and failing to disclose the breach in a timely fashion.

59. The consequences associated with the Equifax data breach are significant, and the breach demonstrates that the Company has, by acting with reckless disregard for the security of consumers' personal information that it promised to protect, utterly failed to implement reasonable security measures to protect its users' sensitive personal information, despite the Company being the target of repeated data breaches in the past. As a result of Defendant's reckless conduct and failure to establish and implement basic data security protocols and, despite its knowledge and the warnings of prior data breaches, consumers' personal information is now in the hands of criminals, regardless of whether they knew they were an Equifax customer in the first place, subjecting

[47] Brian Hamrick, *The dark web: A trip into the underbelly of the internet*, WLWT News, Feb. 9, 2017 8:51 PM, http://www.wlwt.com/article/the-dark-web-a-trip-into-the-underbelly-of-the-internet/8698419 (last visited Sept. 13, 2017).

Plaintiffs and the Class to the serious risk of identity theft in a wide variety of forms.

60. Reports already suggest that criminal activity for fraudulent account takeovers has increased in recent months. One fraud prevention company "***saw a 'significant' spike" in account takeover attempts – a 15% increase year-over-year – in the last two months***, suggesting the increased activity could be related to the Equifax breach.[48]

61. Plaintiffs have expended or will be required to expend substantial time and sums of money as a direct result of the data breach. Plaintiffs, and other Class members who do the same, should be compensated by Equifax for their expenses in light of Equifax's failure to adequately secure consumers' personal information.

62. Additionally, Plaintiffs and Class members suffered and continue to suffer imminent injury arising from the substantially increased risk of future fraud, identity theft or improper use of their personal information by criminals who have or imminently will misuse such information by virtue of Equifax's data breach. Further, Plaintiffs and Class members have a continued interest in ensuring that their personal information, which continues to remain in the control of Equifax, is protected and otherwise safeguarded from future breaches.

V. CLASS ACTION ALLEGATIONS

63. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 ("Rule 23") on behalf of themselves and a class of other similarly situated individuals (the "Class"), as defined specifically below:

> All persons within the United States whose personal information was accessed, compromised or stolen following the data breach that Equifax announced in a press release on September 7, 2017.

[48] Nicole Sinclair, *Expert: Fraudsters may already be trying to use breached Equifax data, Yahoo! Finance*, Sept. 12, 2017, https://finance.yahoo.com/news/expert-fraudsters-may-already-trying-use-breached-equifax-data-172337733.html.

64. Plaintiffs also bring this action under the statutory and common laws of their state of residence on behalf of themselves and classes of other similarly situated individuals, as defined as:

> All persons within the state of Florida whose personal information was accessed, compromised or stolen following the data breach that Equifax announced in a press release on September 7, 2017.

65. Excluded from the Class is Defendant; any person who is an officer, director, partner or controlling person of Defendant, including any of its subsidiaries or affiliates; any entity in which Defendant has a controlling interest; and the legal representatives, heirs, successors and assigns of any such excluded person or entity.

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

67. **Numerosity**. Equifax has stated publicly that approximately 143 million U.S. consumers were affected by this data breach. Joinder is therefore impracticable and the numerosity requirement of Rule 23 is easily satisfied here.

68. **Commonality**. Plaintiffs' and Class members' claims raise predominately common factual and legal questions that can be answered for all Class members through a single class-wide proceeding. For example, to resolve any Class member's claims, it will be necessary to answer the following questions, and the answer to each of these questions will necessarily be the same for each Class member.

a. whether Defendant owed a duty of care to Plaintiffs and the Class with respect to the security of their personal information;

b. whether Defendant acted with reckless disregard for the safety and security of the personal information it promised to protect by failing to establish

appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against known and anticipated threats or hazards to the security and integrity of these records;

c. whether the Defendant's conduct was reckless or intentional;

d. whether Defendant acted appropriately in securing Plaintiffs and Class members' personal information;

e. whether Defendant violated Florida Deceptive and Unfair Trade Practices Act;

f. whether Defendant violated Florida law by failing to timely disclose the data breach to Florida residents; and

g. whether Plaintiffs and Class members are entitled to damages, declaratory and/or injunctive relief.

69. **Typicality**. Plaintiffs' claims are typical of the claims of the members of the Class. Among other things, Plaintiffs and Class members provided personal information that was stored on Defendant's systems. In addition, Plaintiffs' claims are typical of Class members' claims as each arises from the same data breach and the same alleged reckless conduct on the part of Equifax in handling the Class members' personal information.

70. **Adequacy**. Plaintiffs will adequately represent the proposed Class members. They have retained counsel competent and experienced in class action and privacy litigation and intend to pursue this action vigorously. Plaintiffs have no interests contrary to or in conflict with the interests of Class members.

71. In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual members and a class action is

superior to individual litigation. Plaintiffs know of no difficulty to be encountered in the management of this action that would preclude its maintenance as a class action.

COUNT I
Violation of Florida Deceptive Trade and Unfair Practices Act (F.S. § 501.204, *et seq*.)

72. Plaintiffs incorporate the above allegations by reference.

73. Florida Statutes § 501.204 ("FDUPTA") makes unlawful any "[d]eceptive acts or practices in the conduct of any business, trade or commerce in the State Florida".

74. By reason of the conduct alleged herein, Equifax engaged in deceptive acts and practices within the meaning of the FDUPTA.

75. Equifax stored the personal information of Plaintiffs and Class members in Equifax's consumer information databases. Equifax represented to Plaintiffs and Class members that their personal information was secure and would remain private. Equifax violated FDUPTA by misleadingly providing on its website that, e.g., "[w]e limit access to your personal information," "[w]e are committed to protecting the security of your information through procedures and technology designed for this purpose," and "[w]e have reasonable physical, technical and procedural safeguards to help protect your personal information."

76. Further, even without these representations, Plaintiffs and Class members were entitled to, and did, assume Equifax would take appropriate measures to keep their personal information safe. Equifax did not disclose at any time that Plaintiffs' personal information was vulnerable to hackers because Equifax's data security measures were inadequate and outdated.

77. Equifax knew or should have known it did not employ reasonable measures that would have kept Plaintiffs' and the other Class members' personal and financial information secure and prevented the loss or misuse of Plaintiffs' and the other class members' personal and

financial information.

78. Equifax's representations that it would secure and protect the personal and financial information of Plaintiffs and Class members were facts that reasonable persons could be expected to rely upon when deciding whether to conduct business with Equifax. Equifax's misrepresentations and omissions are likely to mislead and did materially mislead Plaintiffs and other reasonable consumers.

79. Equifax violated FDUPTA (§501.204 *et. seq*.) by misrepresenting, both by affirmative conduct and by omission, the safety of its many systems and services, specifically the security thereof, and its ability to safely store Plaintiffs' and Class members' personal information. Equifax also violated FDUPTA (§ 501.204 *et seq.*) by failing to immediately notify Plaintiffs and the other Class members of the data breach. If Plaintiffs and Class members had been notified in an appropriate fashion, they could have taken precautions to safeguard their personal information.

80. Equifax also violated its commitment to maintain the confidentiality and security of the personal information of Plaintiffs and Class members, and failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security.

81. Plaintiffs and the other Class members suffered injury in fact and lost money or property as the result of Equifax's failure to secure Plaintiffs' and Class members' personal information contained in Equifax's servers and/or databases. In particular, Plaintiffs and Class members have suffered or are in imminent risk of suffering from forged credit applications and tax returns; improper or fraudulent charges to their credit/debit card accounts; hacked emails; and other similar harm, all as a result of the Equifax data breach. In addition, their personal information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiffs and Class

members have also suffered or are in imminent risk of suffering consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

82. As a result of Equifax's violations of FDUPTA (§ 501.204 *et seq.*), Plaintiffs and the other Class members are entitled to monetary damages, a declaratory judgment, injunctive relief and attorneys' fees pursuant to Fla. Stat. § 501.2105.

COUNT II
Negligence

83. Plaintiffs incorporate the above allegations by reference.

84. By maintaining their personal information in a database that was accessible through the Internet, Equifax owed Plaintiffs and Class members a duty of care to employ reasonable security measures to protect this information.

85. Defendant, with reckless disregard for the safety and security of consumers' personal information it was entrusted with, breached the duty of care owed to Plaintiffs and the Class by failing to implement reasonable security measures to protect consumers' sensitive personal information. In failing to employ these basic and well-known Internet security measures, Equifax departed from the reasonable standard of care and violated its duty to protect Plaintiffs' and Class members' personal information.

86. The unauthorized access to Plaintiffs' and Class members' personal information was reasonably foreseeable to Equifax, particularly considering that the method of access is widely known in the consumer credit reporting and data security industry.

87. Neither Plaintiffs nor other Class members contributed to the security breach or Equifax's employment of insufficient security measures to safeguard personal information.

88. As a direct and proximate cause of Equifax's reckless conduct, Plaintiffs and Class

members suffered injury through the public disclosure of their personal information, the unauthorized access of certain credit dispute documents containing additional personal information, and through the heightened risk of unauthorized persons stealing additional personal information. Plaintiffs and Class members have also incurred the cost of taking measures to identify and safeguard accounts put at risk by disclosure of the personal information stolen from Equifax, including placing a security freeze on their credit file.

COUNT III
Willful Violation of the Fair Credit Reporting Act
15 U.S.C. § 1681, *et seq.*

89. Plaintiffs incorporate the above allegations by reference.

90. Plaintiffs and Class members are individual consumers as that term is defined in the Fair Credit Reporting Act ("FCRA"). 15 U.S.C. §1681a(c).

91. A "consumer reporting agency" under the FCRA means "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).

92. Equifax is a consumer reporting agency under the FCRA because 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 for monetary compensation.

93. The FCRA requires Equifax, as a consumer reporting agency, 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).

94. 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). The data compromised as part of the Equifax security breach 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.

95. Because Equifax is a consumer reporting agency, it 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 Plaintiffs' and Class members' personal information. Equifax violated §1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed herein.

96. Specifically, Equifax disclosed Class members' 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.

97. 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, the fact that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, Equifax touts that as part of its core business it helps consumers manage and protect their personal information; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

98. Moreover, Equifax 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. 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.

99. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and Class members' personal information for no permissible purposes under the FCRA.

COUNT V
Negligent Violation of the Fair Credit Reporting Act
15 U.S.C. § 1681, *et seq.*

100. Plaintiffs incorporate the above allegations by reference.

101. Equifax negligently failed to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, the fact that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an industry leader touting that as part of its core business it helps consumers manage and protect their personal information, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

102. Equifax's negligent conduct provided a means for hackers, criminals and other unauthorized intruders to obtain Plaintiffs' and Class members' personal information and consumer reports for no permissible purposes under the FCRA.

103. Plaintiffs and the Class members have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiffs and each of the Class member are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. §1681o(a)(1).

104. Plaintiffs and 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 VI
Declaratory Relief

105. Plaintiffs incorporate the above allegations by reference.

106. There is an active case and controversy among Plaintiffs on the one hand, and Equifax on the other.

107. Plaintiffs seek declaratory relief under 28 U.S.C. § 2201, declaring that:

a. Equifax owed, and continues to owe, a legal duty to safeguard and protect Plaintiffs' and Class members' personal information, and timely notify them about the data breach

announced September 7, 2017;

b. Equifax breached, and continues to breach, such legal duties by failing to safeguard and protect Plaintiffs' and Class members' personal information;

c. Equifax's breach of its legal duties directly and proximately caused the data breach announced on September 7, 2017 and the resulting damages, injury, or harm suffered by Plaintiffs and Class members; and

d. To the extent that Plaintiffs' claims herein are covered by Equifax's Terms of Use or privacy policies, the limitation of liability, arbitration and class action waiver provisions are unenforceable because they are against public policy and both procedurally and substantively unconscionable.

108. Further, a declaration from the Court ordering Equifax to stop its illegal practices is required.

109. As a result of the data breach and Equifax's duties to safeguard and protect Plaintiffs' and Class members' personal information, Equifax and Equifax's security measures were, and continue to be, wholly inadequate. Equifax disputes these contentions.

110. Moreover, Plaintiffs are in doubt as to whether Equifax's Terms of Use apply to their claim and whether, if so, the limitation of liability clause therein is lawful and enforceable under Florida law. There is a bona fide dispute between the parties hereto, and Plaintiffs have and do raise justiciable issues as to the existence or non-existence of their rights, powers, obligations, and legal relations with Equifax by virtue of the Terms of Use and privacy policies, this complaint, and the applicable statutes and rules of this state.

111. Plaintiffs are in doubt as to their rights, powers, obligations, and legal relations and there is an actual and present need for a declaratory judgment as to the issues set forth herein.

PRAYER
FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class and state law classes, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiffs as representatives of the Class, and appointing his counsel as Class Counsel;

B. Awarding damages, including, but not limited to, compensatory, statutory, and punitive damages, to Plaintiffs and Class members in an amount to be determined at trial;

C. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class;

D. Providing for declaratory relief as requested above;

E. Awarding Plaintiffs and the Class their reasonable litigation expenses and attorneys' fees;

F. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and

G. Awarding such other and further relief as equity and justice may require.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury for all issues so triable.

DATED: September 20th, 2017.

HABER SLADE, P.A.
Attorneys for Plaintiffs
201 S. Biscayne Blvd., Suite 1205
Miami, Florida 33131
Tel: (305) 379-2400
Fax: (305) 379-1106
dbhpaservice@dhaberlaw.com

/s/ Roger Slade
ROGER SLADE, ESQ.
Fla. Bar No. 41319
rslade@dhaberlaw.com
REBECCA NEWMAN CASAMAYOR, ESQ.
Fla Bar. No. 99070
rcasamayor@dhaberlaw.com
cpla@dhaberlaw.com

STEVEN F. SAMILOW, P.A.
Co-Counsel for Plaintiffs
7777 Glades Road
Suite 100
Boca Raton, Florida 33434-4150
Tel: (561) 245-4633
samilow@aol.com

/s/ Steven F, Samilow
STEVEN F. SAMILOW, ESQ.
Fla Bar No.: 769142
samilow@aol.com