UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

WILLY GRANADOS, individually and on behalf of all others similarly situated, Plaintiff, v. LENDINGTREE, LLC, Defendant.	Case No. 3:22-cv-504 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Willy Granados ("Plaintiff"), individually and on behalf of all others similarly situated, by and through Plaintiff's undersigned attorneys, brings this action ("Action") against Defendant LendingTree, LLC ("LendingTree" or "Defendant"), and alleges the following upon information and belief, except as to those allegations concerning Plaintiff, which are based upon personal knowledge.

INTRODUCTION

1. This Action arises out of the 2022 data breach (the "Data Breach") that was perpetrated against Defendant LendingTree, LLC, an online lending marketplace. The Data Breach resulted in unauthorized access and exfiltration of highly sensitive and personal information (the "Private Information").

2. As a result of the Data Breach, Plaintiff and approximately 200,000 current, former, or prospective customers who utilized LendingTree's services (the "Class Members") suffered present injury and damages in the form of identity theft, out-of-pocket expenses, and the value of the

time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

3. The Private Information compromised in the Data Breach includes Social Security numbers, dates of birth, full names, and street addresses.

4. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

5. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks.

6. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information risked a cyberattack.

7. Plaintiff's and Class Members' identities are now at considerable risk because of Defendant's negligent conduct since the Private Information that LendingTree collected and maintained is now in the hands of data thieves.

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes, including but not limited to fraudulently applying for unemployment benefits, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits (including unemployment or COVID relief benefits), filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and providing false information to police during an arrest.

9. Plaintiff's and Class Members' Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its failure to adequately protect the Private Information of its current, former, and prospective customers.

10. As a result of the Data Breach, Plaintiff and Class Members are exposed to a heightened present and imminent risk of fraud and identity theft. As a result of Defendant's actions and inactions, as set forth herein, Plaintiff and Class Members must now and in the future closely monitor their financial accounts and information to guard against identity theft, among other issues.

11. Plaintiff and Class Members have and may in the future incur actual monetary costs, including but not limited to the cost of purchasing credit monitoring services, credit freezes, credit reports or other protective measures to deter and detect identity theft.

12. Plaintiff and Class Members have and may in the future expend time mitigating the effects of the Data Breach, including time spent dealing with actual or attempted fraud and identity theft.

13. By his Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Accordingly, Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's negligence and failure to: (i) adequately protect its customer's Private Information, (ii) warn its current, former, and potential customers of its inadequate information security practices, and (iii) effectively monitor its data systems for security vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

15. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to

Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

16. Plaintiff Willy Granados is, and at all relevant times has been, a resident of the state of California. He has used LendingTree's services. Plaintiff received a copy of the "Notice of Data Breach" letter dated June 29, 2022 from Defendant LendingTree. The letter informed Plaintiff that, "[o]n June 3, 2022, LendingTree determined that a code vulnerability likely resulted in the unauthorized disclosure of some sensitive personal information." LendingTree further stated that it believed "the unauthorized disclosure began in mid-February 2022."

17. Defendant LendingTree is a for-profit Delaware limited liability company with its headquarters and principal place of business at 1415 Vantage Park Drive, Suite 700, Charlotte, North Carolina 28203.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

19. This Court has personal jurisdiction over Defendant because Defendant does substantial business in this District, is headquartered in this District, and maintains its principal place of business in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendant resides within this judicial district, does substantial

business in this District, is headquartered in this District, and maintains its principal place of business in this District.

FACTUAL ALLEGATIONS

LendingTree's Business

21. Defendant LendingTree describes itself on its website as "a lot more than mortgages. [LendingTree] [is] an online loan marketplace for various financial borrowing needs including auto loans, small business loans, personal loans, credit cards, and more. [LendingTree] also offer[s] comparison shopping services for autos and educational programs. Together, these services serve as an ally for consumers who are looking to comparison shop among multiple businesses and professionals who will compete for their business."[1]

22. Upon information and belief, in the ordinary course of doing business with Defendant, Defendant collects sensitive Private Information from customers and potential customers such as:

- Full Name;
- Street Address;
- Social Security number;
- Date of birth;

23. In the course of collecting Private Information from customers and potential customers, including Plaintiff and Class Members, Defendant promises to provide confidentiality and security for customers' and potential customers' Private Information, including by promulgating and placing privacy policies on its website.

LendingTree's Privacy Policy

24. In the LendingTree Privacy Policy (hereinafter "Privacy Policy"), which is effective

[1] https://www.lendingtree.com/press/, (last visited Sep. 14, 2022).

as of February 5, 2021 and provided on Defendant's website, Defendant states that it is "committed to maintaining your confidence and trust as it relates to the privacy and usage of your information."[2]

25. Further in the Privacy Notice, Defendant promises to protect consumers' Private Information and that it uses "physical, electronic, and procedural measures designed to safeguard your information from unauthorized access and disclosure."[3]

26. However, Defendant failed to protect and safeguard Plaintiff's and Class Members' Private Information.

LendingTree's Terms of Use Agreement

27. LendingTree has posted its "Terms of Use Agreement" online, which purports to bind LendingTree's users as follows: "By using this website, you are entering into a legal agreement to abide by the terms of use you see here, and you are agreeing that you have read and fully understand these terms of use."[4]

28. This Terms of Use Agreement, last updated January 1, 2020, purports to limit LendingTree's liability to $100 in the event that users' personal information is stolen from LendingTree, regardless of whether LendingTree is at fault for the theft. Specifically, the Limitation on Damages section of the LendingTree Terms of Use Agreement provides in part:

> LENDINGTREE'S LIABILITY, IF ANY, SHALL BE LIMITED TO DIRECT AND FORESEEABLE DAMAGES, WHICH SHALL NOT EXCEED [$100.00]. UNDER NO CIRCUMSTANCES SHALL LENDINGTREE BE LIABLE FOR . . . LOSS OF OR DAMAGE TO DATA, . . . THESE LIMITATIONS AND EXCLUSIONS APPLY EVEN IF THIS REMEDY DOES NOT FULLY COMPENSATE YOU FOR ANY LOSSES OR FAILS OF ITS ESSENTIAL PURPOSE OR IF WE KNEW OR SHOULD

[2] *LendingTree Privacy Policy*, LendingTree, available at https://www.lendingtree.com/legal/privacy-policy/ (last visited Sep. 14, 2022).
[3] *Id*.
[4] *LendingTree Terms of Use Agreement*, LendingTree, available at https://www.lendingtree.com/legal/terms-of-use/ (last visited Sep. 14, 2022).

HAVE KNOWN ABOUT THE POSSIBILITY OF THE DAMAGES. [5]

LendingTree Admits to Massive Data Breach

29. On June 29, 2022, LendingTree sent a Notice of Data Breach letter to its users. The letter stated that, "[o]n June 3, 2022, LendingTree determined that a code vulnerability likely resulted in the unauthorized disclosure of some sensitive personal information."[6] LendingTree further stated that it believed "the unauthorized disclosure began in mid-February 2022."[7]

30. The Notice of Data Breach further states that '[t]he types of impacted information included name, social security number, date of birth, and street address."[8]

31. The Notice of Data Breach attempts to reassure consumers by stating that "[t]he vulnerability in the code no longer exists, and [LendingTree] [is] working to implement additional security measures to protect consumers who visit our online interfaces."[9]

32. The Notice of Data Breach includes an offer from LendingTree for two years' worth of free credit monitoring, but only gives consumers a mere 90 days to sign up for such services.[10]

33. Missing from the Notice of Data Breach is any explanation of what "code vulnerability" means.[11] Also missing is any explanation as to who took the data and how the data was taken.[12]

34. At this time, Defendant has not indicated exactly how long the unauthorized third-

---

[5] *Id*.
[6] *Notice of Data Breach*, LendingTree, June 29, 2022.
[7] *Id*.
[8] *Id*.
[9] *Id*.
[10] *Id*.
[11] April Strauss, Esq., Lending Tree Data Breach, Sensitive Information Potentially Disclosed in Hack, available at Lending Tree Data Breach, Sensitive Information Potentially Disclosed in Hack • LegalScoops (last visited Sep. 14, 2022).
[12] *Id*.

party had unfettered access to sensitive, protected, and confidential customer information stored on Defendant's network, such as Plaintiff's and Class Members' Private Information. Defendant only offers a vague nearly four-month period from mid-February 2022-June 3, 2022. Had Defendant taken its data security obligations more seriously, Defendant would have discovered and stopped the unauthorized intrusion sooner. Furthermore, there has been no explanation as to why LendingTree waited nearly one month after discovering the Data Breach on June 3, 2022 to notify consumers of such breach, which it only did on June 29, 2022.

35. To make matters worse, Private Information stolen during the Data Breach has been posted online since on or before June 18, 2022.[13] The digital privacy advocacy group Restore Privacy reviewed the data posted online and determined that it contains data for 200,643 consumers.[14] Their review also found that the online posting contains the following types of data for each customer: email address, name (first and last), physical address, phone number, IP address, data and time of loan form submission, loan type that the applicant is seeking, home description, credit profile score, property use, military status, and price.[15] This is considerably more Private Information than LendingTree disclosed was stolen in the Notice of Data Breach, which listed only name, Social Security number, date of birth, and street address.[16]

36. Upon information and belief, the cyberattack was targeted at Defendant due to its status as a leading lending company that collects and maintains valuable Private Information, such as Social Security numbers and financial information.

---

[13] Sven Taylor, *Hacker Leaks Database Claiming to be from LendingTree*, June 21, 2022, available at Hacker Leaks Database Claiming to be from LendingTree | RestorePrivacy (last visited Sep. 14, 2022).
[14] *Id*.
[15] *Id*.
[16] *Notice of Data Breach*, LendingTree, June 29, 2022.

37. The targeted cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the Private Information of current, former, and prospective customers, like Plaintiff and the Class Members.

38. Because of this targeted cyberattack, data thieves were able to gain access to Defendant's servers and subsequently access and exfiltrate the protected Private Information of Plaintiff and Class Members.

39. The files accessed by this incident contained the following information, among other types: names, dates of birth, Social Security numbers, and street addresses.

40. There is no indication that the Private Information contained in the stolen files was encrypted.

41. Plaintiff's Private Information was accessed and stolen in the Data Breach. Plaintiff further believes his stolen Private Information was subsequently sold on the Dark Web.

42. Defendant's offer of 24 months of complimentary credit monitoring services is an acknowledgment by LendingTree that the impacted individuals are subject to a present and ongoing threat of fraud and identity theft.

43. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

44. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation, and mutual understanding, that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

Defendant Was Aware of the Risks of a Data Breach

45. LendingTree was aware of the risks of a cyberattack since it had experienced data breaches at least twice before – in 2008[17] and again in January 2022.[18]

46. The Data Breach and LendingTree's failure to timely detect it indicates that LendingTree failed to adequately implement measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of at least 200,643 consumers, including Plaintiff and Class Members.

Defendant Failed to Comply with FTC Guidelines

47. The Federal Trade Commission ("FTC") has promulgated numerous guidelines for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

48. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

---

[17] Sven Taylor, *Hacker Leaks Database Claiming to be from LendingTree*, June 21, 2022, available at Hacker Leaks Database Claiming to be from LendingTree | RestorePrivacy (last visited Sep. 14, 2022).

[18] https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/JulyYear-to-date-Report.pdf

49. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

50. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

51. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

52. Defendant was at all times fully aware of its obligation to protect the Private Information of current, former, and prospective customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

53. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

54. Best cybersecurity practices that are standard in Defendant's industry include

encrypting files; installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

55. Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

56. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyberattack and causing the Data Breach.

Defendant's Breach

57. LendingTree breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. LendingTree's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect current, former, and prospective customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and

e. Failing to adhere to industry standards for cybersecurity.

58. LendingTree negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

59. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with LendingTree.

The Value of Private Information to Cyber Criminals and Increased Risk of Fraud and Identity Theft to Consumers

60. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

61. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[19]

62. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult

[19] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), available at https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last visited Sep. 14, 2022).

for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[20]

63. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

64. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[21]

65. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have

[20] *Identity Theft and Your Social Security Number*, Social Security Administration (2018), available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sep. 14, 2022).
[21] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Sep. 14, 2022).

> records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[22]

66. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential Private Information to mimic the identity of the user. The personal data of Plaintiff and Members of the Classes stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiff and the Classes.

67. Stolen personal data of Plaintiff and Members of the Classes represents essentially one-stop shopping for identity thieves.

68. The FTC has released its updated publication on protecting Private Information for businesses, which includes instructions on protecting Private Information, properly disposing of Private Information, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

69. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According

[22] *Supra*, note 20.

to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [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.[23]

70. Companies recognize that Private Information is a valuable asset. Indeed, Private Information is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other Private Information on a number of Internet websites. The stolen personal data of Plaintiff and members of the Classes has a high value on both legitimate and black markets.

71. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment or COVID-19 relief benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

72. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's current, former, and prospective customers whose Social Security numbers have been compromised now face a present and imminent risk of

[23] *See* U.S. Gov. Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007) at 29, available at https://www.gao.gov/new.items/d07737.pdf (last visited Aug. 19, 2021).

identity theft and other problems associated with the disclosure of their Social Security numbers and will need to monitor their credit and tax filings for an indefinite duration.

73. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, name, and date of birth.

74. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

75. According to a recent article in the New York Times, cyber thieves are using illegally obtained driver's licenses to submit and fraudulently obtain unemployment benefits.[24] An individual may not know that his or her driver's license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

Plaintiff Willy Granados's Experience

76. Plaintiff Willy Granados opened his customer account with Defendant in or about March 2022 and was required to provide, among other things, his full name, date of birth, Social Security number, and street address.

77. On or about June 29, 2022, Plaintiff Granados, and the public, was first notified of the Data Breach by LendingTree and that cybercriminals had illegally accessed and stole confidential

[24] *How Identity Thieves Took My Wife for a Ride*, New York Times, (April 27, 2021) https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited Sep. 14, 2022).

customer data from over 200,000 LendingTree customer accounts.

78. As a direct and proximate result of the breach, Plaintiff Granados has made reasonable efforts to mitigate the impact of the breach, including but not limited to: discussing the breach with his friends and consulting with legal counsel. This is valuable time Plaintiff Granados otherwise could have or would have spent on other activities, including but not limited to, work and/or recreation.

79. Plaintiff Granados is very concerned about identity theft, his banking account and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

80. Plaintiff Granados suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

81. As a result of the Data Breach, Plaintiff Granados anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff's and Class Members' Damages

82. To date, Defendant has done absolutely nothing to provide Plaintiff and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach.

83. Defendant has only offered inadequate identity monitoring services. Defendant places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for

that service, as opposed to automatically enrolling all victims of this cybercrime. In addition, Defendant only offers these services for two years, even though experts agree that the effects of such a data breach can often be felt by victims for around seven years.

84. Plaintiff's and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

85. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members are in imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

86. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

87. Plaintiff and Class Members face a present and substantial risk of out-of-pocket fraud losses such as loans opened in their names, government benefits fraud, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

88. Plaintiff and Class Members face a present and substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

89. Plaintiff and Class Members have and may continue to incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

90. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

91. Plaintiff and Class Members have spent and will continue to spend significant amounts

of time to monitor their financial accounts for misuse. Indeed, Defendant's own Notice of Data Breach includes a list of Recommended Steps to help Protect your Information."[25]

92. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered 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 relating to:

a. Finding fraudulent charges, loans, and/or government benefit claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with credit reporting agencies;

d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;

e. Contacting financial institutions and closing or modifying financial accounts;

f. Closely reviewing and monitoring Social Security numbers, bank accounts, and credit reports for unauthorized activity for years to come.

93. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

94. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at an imminent and increased risk of future

[25] *Notice of Data Breach*, LendingTree, June 29, 2022.

harm.

95. To date, Defendant has done absolutely nothing to provide Plaintiff and Class members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach.

96. Defendant has only offered inadequate identity monitoring services, and it is unclear whether that credit monitoring was only offered to certain affected individuals (based upon the type of data stolen), or to all persons whose data was compromised in the Data Breach. What is more, Defendant places the burden squarely on Plaintiff and Class members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this cybercrime.

CLASS ACTION ALLEGATIONS

97. Plaintiff brings this nationwide class action pursuant to rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class:

> All current, former, and prospective LendingTree customers residing in the United States whose Private Information was compromised in the Data Breach announced by Defendant on or about June 2022 (the "Nationwide Class").

98. The California Subclass is defined as follows:

> All current, former, and prospective LendingTree customers residing in California whose Private Information was compromised in the Data Breach announced by Defendant on or about June 2022 (the "Nationwide Class").

99. The California Subclass is referred to herein as the "Statewide Subclass" and together with the Nationwide Class, are collectively referred to herein as the "Classes."

100. Excluded from the Classes are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

101. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

102. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendant has identified hundreds of thousands of current, former, and prospective customers whose Private Information may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendant's records.

103. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual members of the Classes. These include:

a. When Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Classes to exercise due care in collecting, storing, safeguarding and/or obtaining their Private Information;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the Private Information of Plaintiff and Members of the Classes;

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of Private Information belonging to Plaintiff and Members of the Classes;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep the Private Information of Plaintiff and Members of the Classes secure and to prevent loss or misuse of that Private Information;

g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiff's and Members of the Classes' damages;

i. Whether Defendant violated the law by failing to promptly notify Plaintiff and Members of the Classes that their Private Information had been compromised;

j. Whether Defendant violated the consumer protection statute invoked below; and

k. Whether Plaintiff and the other Members of the Classes are entitled to credit monitoring and other monetary relief;

104. **Typicality**: Plaintiff's claims are typical of those of the other Members of the Classes because all had their Private Information compromised as a result of the Data Breach due to Defendant's misfeasance.

105. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff's Counsel are competent and experienced in litigating privacy-related class actions.

106. **Superiority and Manageability**: Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual member of the Classes are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

107. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole and as to the

Subclass as a whole.

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

a. Whether Defendant owed a legal duty to Plaintiff and Members of the Classes to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Members of the Classes to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether members of the Classes are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

COUNT I

Negligence
(On Behalf of Plaintiff, the Nationwide Class, and the Statewide Subclass)

109. Plaintiff repeats and incorporates the allegations above as if fully set forth herein.

110. Defendant owed a common law duty to Plaintiff and Members of the Classes to exercise reasonable care in obtaining, using, and protecting their Private Information from unauthorized third parties.

111. The legal duties owed by Defendant to Plaintiff and Members of the Classes include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information of Plaintiff and Members of the Classes in its possession;

b. To protect the Private Information of Plaintiff and Members of the Classes in its possession using reasonable and adequate security procedures 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, including promptly notifying Plaintiff and Members of the Classes of the Data Breach.

112. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect personal information.

113. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiff and Members of the Classes are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect personal information and by not complying with industry standards.

114. Defendant breached its duties to Plaintiff and Members of the Classes. Defendant knew or should have known the risks of collecting and storing Private Information and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging in the past five years.

115. Defendant knew or should have known that its security practices did not adequately safeguard the Private Information belonging to the Plaintiff and Members of the Classes.

116. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the Private Information of Plaintiff and Members of the Classes from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff and Members of the Classes during the period it was within Defendant's possession and control.

117. Defendant breached the duties it owed to Plaintiff and Members of the Classes in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect current, former, and prospective customers' Private Information, including Plaintiff and Members of the Classes, and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards prior to the Data Breach; and

c. Failing to act despite knowing or having reason to know that its systems were vulnerable to attack.

118. Due to Defendant's conduct, Plaintiff and Members of the Classes are entitled to credit monitoring. Credit monitoring is reasonable here. The Private Information taken can be used for identity theft and other types of financial fraud against Plaintiff and Members of the Classes.

119. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach.[26] Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

120. As a result of Defendant's negligence, Plaintiff and Members of the Classes suffered injuries that may include: (i) the lost or diminished value of Private Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing scams and reviewing and monitoring sensitive accounts; (iv) the present and continued risk to their Private Information, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; and (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Members of the Classes, including ongoing credit monitoring.

[26] In the Equifax data breach, for example, Equifax agreed to free monitoring of victims' credit reports at all three major credit bureaus for four years, plus $1 million of identity theft insurance. For an additional six years, victims can opt for free monitoring by one credit bureau, Equifax. In addition, if a victim's child was a minor in May 2017, he or she is eligible for a total of 18 years of free credit monitoring under the same terms as for adults.

121. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and the members of the Classes suffered was the direct and proximate result of Defendant's negligent conduct.

COUNT II

Negligence *Per Se*
(On Behalf of Plaintiff, the Nationwide Class, and the Statewide Subclass)

122. Plaintiff repeats and incorporates the allegations above as if fully set forth herein.

123. 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 Defendant's, of failing to use reasonable measures to protect personal information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

124. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect personal information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of personal information it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Members of the Classes due to the valuable nature of the personal information at issue in this case—including Social Security numbers.

125. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

126. Plaintiff and Members of the Classes are within the classes of persons that the FTC Act was intended to protect.

127. The harm that occurred as a result of the 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 its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Members of the Classes.

128. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Members of the Classes have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the present and continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of its current, former, and prospective customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Members of the Classes.

129. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Members of the Classes have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

COUNT III

Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200*, et seq*. – Unlawful Business Practices
(On Behalf of Plaintiff and the Statewide Subclass)

130. Plaintiff repeats and incorporates the allegations above as if fully set forth herein.

131. Defendant has violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Statewide Subclass.

132. Defendant engaged in unlawful acts and practices with respect to its services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Statewide Subclass Members' Private Information with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Statewide Subclass Members' Private Information in an unsecure environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to take reasonable methods of safeguarding the Private Information of Plaintiff and the Statewide Subclass Members.

133. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach to California Subclass Members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

134. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff and the Statewide Subclass Members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Statewide Subclass Members' legally protected interest in the confidentiality and privacy of their Private Information, nominal damages, and additional losses as described above.

135. Defendant knew or should have known that Defendant's computer systems and data security practices were inadequate to safeguard Statewide Subclass Members' Private Information and that the risk of a data breach or theft was highly likely, especially given Defendant's inability to adhere to basic encryption standards and data disposal methodologies. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Statewide Subclass.

136. Statewide Subclass Members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and Statewide Subclass Members of money or property that Defendant may have acquired by means of Defendant's unlawful and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT IV

Restitution and Unjust Enrichment
(On Behalf of Plaintiff, the Nationwide Class, and the Statewide Subclass)

137. Plaintiff repeats and incorporates the allegations above as if fully set forth herein.

138. As a result of LendingTree's misleading representations and omissions concerning the adequacy of its data security practices, Plaintiff and the Classes were induced to use LendingTree's services, and to provide LendingTree with their Private Information.

139. LendingTree derived substantial revenues due to Plaintiff and the Classes purchasing and using LendingTree's services and providing LendingTree with their Private Information.

140. In addition, LendingTree saved on the substantial cost of providing adequate data security to Plaintiff and the Classes, although LendingTree's savings came at the expense of the privacy and confidentiality of Private Information belonging to Plaintiff and the Classes.

141. Plaintiff and the Classes have been damaged by LendingTree's actions, and LendingTree has been unjustly enriched thereby. Plaintiff and the Classes are entitled to damages as a result of LendingTree's unjust enrichment, including the disgorgement of all revenue received and costs saved by LendingTree as a result of this conduct.

COUNT V

North Carolina Unfair and Deceptive Trade Practices Act
(On Behalf of Plaintiff and the Nationwide Class)

142. Plaintiff repeats, realleges, and incorporates by reference each of the foregoing paragraphs as if fully set forth herein.

143. Defendant has violated N.C.G.S. § 75.1-1 *et seq.*., by engaging in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" with respect to the services provided to the Nationwide Class.

144. Defendant engaged in unlawful acts and practices with respect to its services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Nationwide Class Members' Private Information with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Nationwide Class Members' Private Information in an unsecure environment.

145. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach to Nationwide Members in a timely and accurate manner, which caused customers of the Defendant greater harm.

146. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff and the Nationwide Class Members were injured and lost money or property, including but not limited to the price received by Defendant for the services, the loss of Nationwide Class Members' legally protected interest in the confidentiality and privacy of their Private Information, nominal damages, and additional losses as described above.

147. Defendant knew or should have known that Defendant's computer systems and data security practices were inadequate to safeguard Nationwide Class Members' Private Information and that the risk of a data breach or theft was highly likely, especially given Defendant's inability to adhere to basic encryption standards and data disposal methodologies. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nationwide Class.

148. Nationwide Class Members seek relief under N.C.G.S. § 75.1-1 *et seq.*, including, but not limited to, restitution to Plaintiff and Nationwide Class Members of money or property that Defendant may have acquired by means of Defendant's unlawful and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unlawful and unfair business practices, treble damages, declaratory relief, attorneys' fees and costs and injunctive or other equitable relief.

149. Defendant's actions affected commerce in North Carolina and nationwide.

150. Plaintiff reasonably relied upon Defendant adequately protecting Plaintiff's and Nationwide Class Members' Private Information.

151. Plaintiff has been actually damaged as the direct and proximate result of Defendant's unfair competition and unfair and deceptive trade practices.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on his own behalf and on behalf of the proposed Classes respectfully requests that the Court enter an order or judgment against LendingTree including the following:

A. Certification of the action under the Federal Rules of Civil Procedure and appointment of Plaintiff as Class Representative and his counsel of record as Class Counsel;

B. Damages in the amount to be determined at trial;

C. Actual damages, statutory damages, punitive or treble damages, and such other relief as provided by the statutes cited herein;

D. Prejudgment and postjudgment interest on such monetary relief;

E. Equitable relief in the form of restitution and/or disgorgement of all unlawful or illegal profits received by LendingTree as a result of the unfair, unlawful, and/or deceptive conduct alleged herein;

F. Equitable relief from any provisions of LendingTree's Terms of Use Agreement that improperly seek to limit LendingTree's liability to Plaintiff and the Classes for the acts discussed herein;

G. Declaratory relief pursuant to California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* and N.C.G.S. § 75.1-1 *et seq.*

H. Provision of credit monitoring services to Plaintiff and the Classes;

I. The costs of bringing this action, including reasonable attorneys' fees; and

J. All other relief to which Plaintiff and members of the proposed Classes may be entitled at law or in equity, and which the Court deems just and proper.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff demands a trial by jury of all the claims asserted that are triable by jury.

Dated: September 27, 2022

By: s/ David M. Wilkerson
Larry S. McDevitt (NC. Bar No. 5032)
David M. Wilkerson (NC. Bar No. 35742)
THE VAN WINKLE LAW FIRM
11 North Market Street
Asheville, NC 28801
Telephone: 828-258-2991
Fax: 828-255-0255
Email: lmcdevitt@vwlawfirm.com
Email: dwilkerson@vwlawfirm.com

Brian P. Murray
GLANCY PRONGAY & MURRAY LLP
230 Park Avenue, Suite 358
New York, NY 10169
Telephone: (212) 682-8340
Fax: (212) 884-0988
bmurray@glancylaw.com

Jon A. Tostrud
TOSTRUD LAW GROUP, P.C.
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: (310) 278-2600
Fax: (310) 278-2640
jtostrud@tostrudlaw.com

Attorneys for Plaintiff