**UNITED STATES DISTRICT COURT**
**FOR THE SOUTHERN DISTRICT OF FLORIDA**

ANDREW GUARINO, individually and on behalf of themselves and all others similarly situated,

Plaintiff,

v.

LAKEVIEW LOAN SERVICING, LLC,

Defendant.

Case No. _____

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

Plaintiff Andrew Guarino ("Plaintiff") alleges upon personal knowledge as to himself and his own actions, and upon information and belief, including the investigation of counsel as follows:

## I. NATURE OF THE ACTION

1. This action arises out of the recent cyber attack and data breach at Lakeview Loan Servicing, LLC ("Defendant" or "LLS") that targeted the information of consumers who utilized LLS for residential mortgage services (the "Data Breach").

2. The Data Breach resulted in unauthorized access to the sensitive data of consumers that used LLS's services. Because of the Data Breach, 2,537,261 Class Members' suffered ascertainable losses inclusive of out-of-pocket expenses and the value of their time incurred to remedy or mitigate the effects of the attack and the present and substantial risk of imminent harm caused by the compromise of their sensitive personal information, including their name, address, loan number, and social security number (and, for some, information connected with a loan application, a loan modification, or other items involving their loan's servicing (hereinafter, the "Personally Identifiable Information" or "PII").

3. To compound matters, LLS's Data Breach occurred from October 27, 2021 through December 7, 2021 and LLS did not ascertain what information was accessed until January 31, 2022.

4. Then LLS sat on the information for over a month – failing to disseminate data breach consumer notifications until March 18, 2022. When a data set that is inclusive of the aforementioned PII is breached, every moment is precious to ensure that that data is not then weaponized against the rightful owner of that data through identity theft. Sitting on this information allowed LLS to dodge responsibility and inevitably worsened the Data Breach victims' chances at weathering the storm that LLS created.

5. As a result of the Data Breach, Plaintiff and Class Members have been harmed – they have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and forever closely monitor their financial accounts to guard against identity theft.

6. Plaintiff and Class Members may also incur out-of-pocket costs, for example, through having to purchase credit monitoring systems, credit freezes, or other protective measures to deter and detect identity theft. Plaintiff seeks to remedy those harms on behalf of himself and all similarly situated persons whose PII was accessed unlawfully during the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement for out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

7. As such, Plaintiff brings this Action against Defendant seeking redress for its unlawful conduct, asserting claims for: (i) negligence, (ii) breach of implied contract, and (iii) breach of fiduciary duty.

## II. JURISDICTION AND VENUE

8. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 Class Members and because the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Moreover, Plaintiff, numerous other Class Members, and Defendants are citizens of different states – namely, the Plaintiff is domiciled in Massachusetts whereas the Defendant is located in Florida.

9. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operated, conducted, engaged in, or carried on a business or business venture in Florida; had offices in Florida; committed tortious acts in Florida; and/or breached a contract in Florida by failing to perform acts required by the contract to be performed in Florida. Defendant is organized under the laws of Florida and headquartered at 4425 Ponce de Leon Blvd, Coral Gables, FL 33146, with its principal place of business in Coral Gables, FL.

10. Venue is proper in this district under 28 U.S.C. §§ 1391(a)(1), 1391(b)(1), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this district, Defendant conducts substantial business in this district, and Defendant resides in this district. Further, Defendant is headquartered and does business in and/or has offices for the transaction of its customary business in this district.

## III. PARTIES

11. Plaintiff Andrew Guarino is a citizen of the Commonwealth of Massachusetts and was harmed by the Data Breach alleged herein.

12. Defendant Lakeview Loan Servicing is a private residential mortgage loan servicer and is a citizen of the State of Florida.

## IV. FACTUAL ALLEGATIONS

### DEFENDANT'S BUSINESS

13. According to the Defendant, LLS is the fourth largest residential mortgage loan servicer in the United States.[1]

14. Specifically, LLS offers four services through their website related to residential mortgage loan servicing: (1) "get cash out," meaning trading home equity in order to get access to cash; (2) lowering payments through interest rate reductions; (3) offering residential mortgages to prospective homebuyers; and (4) servicing loans for residential mortgages.[2]

15. According to LLS's Privacy Policy, "[t]he types of personal information [LLS] collect[s] and share[s] depend[s] on the product or service [the consumer] has with [LLS.] That information include[s]:

a. Social security number and income;

b. Account balances and payment history; and,

c. Credit history and credit scores."[3]

16. Additionally, the Privacy Policy states: "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[4]

---

[1] https://lakeview.com, (last accessed Mar. 31, 2022).
[2] *Id.*
[3] https://lakeview.com/privacy-policy/, (last accessed Mar. 31, 2022).
[4] *Id.*

17. By obtaining, collecting, using and deriving benefits from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting said PII from unauthorized disclosure.

18. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

**THE DATA BREACH**

19. To define data breaches: "a data breach exposes confidential, sensitive, or protected information to an unauthorized person. The files in a data breach are viewed and/or shared without permission."[5]

20. In December 2021, LLS experienced a security incident involving unauthorized access to its file servers.

21. Defendant LLS launched an investigation and determined that an unauthorized individual obtained access to files on its storage servers from October 27, 2021 to December 7, 2021.

22. On January 31, 2022, Defendant finally ascertained what information was accessed in the Breach.

23. However, LLS then sat on the information for over a month – failing to disseminate data breach consumer notifications until March 18, 2022.

24. The Data Breach resulted in unauthorized access to the sensitive data of approximately 2.3 million consumers.

25. The sensitive PII stolen in the Data Breach included Plaintiff's and Class Members' names, addresses, loan numbers, and Social Security numbers.

---

[5] "*How Data Breaches Happen*," KASPERSKY, at https://www.kaspersky.com/resource-center/definitions/data-breach (last accessed Mar. 15, 2022).

26. The Personally Identifiable Information contained in the files accessed in the Data Breach was not encrypted.

27. Plaintiff and Class Members provided their Personally Identifiable Information to Defendant with the reasonable expectation and the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. Defendant's data security obligations were particularly important given the substantial increase in data breaches preceding the date of the breach.

28. Therefore, the increase in such attacks, and the attendant risk of future attacks was widely known to the public and to anyone in the Defendant's industry, including the Defendant itself.

***Securing PII and Preventing Breaches***

29. LLS could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and computer files containing PII.

30. In its notice letters, LLS acknowledged the sensitive and confidential nature of the PII. To be sure, collection, maintaining, and protecting PII is vital to virtually all of LLS's business purposes as a financial services firm. LLS acknowledged through its conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

***The Data Breach was a Foreseeable Risk of which Defendant was on Notice***

31. It is well known that PII, including Social Security numbers and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

32. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[6]

---

[6] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf **(last accessed December 10, 2021)**

33. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being exposed exceeding 100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.[7]

34. The 108 reported financial sector data breaches reported in 2019 exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.[8]

35. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

36. Individuals are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers." There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."

37. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), LLS knew or should have known that its electronic records would be targeted by cybercriminals.

---

[7] ***Id.***
[8] ***Id* at p. 15.**

38. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

39. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, LLS failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

***At All Relevant Times LLS Had a Duty to Plaintiff and Class Members to Properly Secure their Private Information***

40. At all relevant times, LLS had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to *promptly* notify Plaintiff and Class Members when LLS became aware that their PII may have been compromised.

41. LLS's duty to use reasonable security measures arose as a result of the special relationship that existed between LLS, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class entrusted LLS with their PII when they transacted with Defendant.

42. LLS had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, LLS breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

43. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

44. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[9] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[10]

45. The ramifications of LLS's failure to keep its consumers' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security and driver's license numbers, fraudulent use of that information and damage to victims is likely to continue for years.

***The Value of Personally Identifiable Information***

46. The PII of consumers 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.[11] According to the Dark Web Price Index for

---

**[9] 17 C.F.R. § 248.201 (2013).**

**[10] *Id.***

**[11] *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 accessed December 10, 2021).**

2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[12]

47. 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 for an individual to change. The Social Security Administration 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.[13]

48. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. 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.

49. Even then, a new Social Security number may not be effective, as "[t]he 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."[14]

---

[12] ***Dark Web Price Index 2021***, **Zachary Ignoffo, March 8, 2021,** ***available at*****: https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed December 10, 2021).**

[13] **Social Security Administration,** ***Identity Theft and Your Social Security Number*****,** ***available at*****: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed December 10, 2021).**

[14] **Brian Naylor,** ***Victims of Social Security Number Theft Find It's Hard to Bounce Back*****, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed December 10, 2021).**

50. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[15]

51. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[16]

52. Given the nature of LLS's Data Breach, as well as the length of the time LLS's systems were breached and the long delay in notification to Class Members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' PII can easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

53. 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 credit card victims can cancel or close credit and debit card accounts.[17] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

54. To date, LLS has offered its consumers *only two years* of identity monitoring services. The offered services are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

55. The injuries to Plaintiff and Class Members were directly and proximately caused

---

[15] **Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed December 10, 2021).**

[16] ***See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.**

[17] ***See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed December 10, 2021).**

by LLS's failure to implement or maintain adequate data security measures for its current and former customers.

***Defendant Fails to Comply with FTC Guidelines***

56. The Federal Trade Commission ("FTC") has promulgated numerous guides 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.

57. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient 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.[18] 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.[19]

58. The FTC further recommends that companies not maintain PII 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

[18] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Mar. 15, 2022).
[19] *Id.*

on the network; and verify that third-party service providers have implemented reasonable security measures.

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, 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.

60. Defendant failed to properly implement basic data security practices.

61. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Personally Identifiable Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

62. Defendant was at all times fully aware of its obligation to protect the Personally Identifiable Information of its subjects. Defendant was also aware of the significant repercussions that would result from its failure to do so.

63. Several best practices have been identified that at a minimum should be implemented by companies like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

64. Other best cybersecurity practices that are standard in the Defendant's industry include 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.

65. Defendant failed to meet the minimum standards of any of the following 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 all established standards in reasonable cybersecurity readiness.

66. 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 and causing the Data Breach.

***Defendant's Breach***

67. Defendant 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. Defendant'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;

b. Failing to adequately protect consumers' PII;

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

d. Failing to train its employees in the proper handling of data breaches, the protection of PII, and the maintenance of adequate email security practices;

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

f. Failing to adhere to industry standards for cybersecurity.

68. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access LLS's IT systems which contained unsecured and unencrypted PII.

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

***Harm to Consumers***

70. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black- market" for years.

71. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

72. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

73. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the

suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

74. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

75. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he 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."[20] The fraudulent activity resulting from the Data Breach may not come to light for years.

76. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personally Identifiable Information is stolen and when it is used.

77. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, driver's license numbers, and financial account information, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

78. Defendant knew or should have known about these dangers and strengthened its data, IT, and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

[20] Brian Naylor, "*Victims of Social Security Number Theft Find It's Hard to Bounce Back*," NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

***Harm to Plaintiff***

79. Prior to the Data Breach, Mr. Guarino provided his PII to LLS for purposes of obtaining a mortgage.

80. In March of 2022, Plaintiff received Notice of Data Breach Letter from LLS informing him that his full name and social security number were stolen by cyberthieves in the Data Breach. As a result of the Data Breach, LLS directed Plaintiff to take certain steps to protect his PII and otherwise mitigate damages.

81. As a result of the Data Breach and the directives that he received in the Notice Letter, Plaintiff spends approximately several hours per week dealing with the consequences of the Data Breach, including, for example, self-monitoring his bank and credit accounts, as well spending time to verify the legitimacy of the *Notice of Data Breach*, communicating with his bank, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured.

82. Plaintiff is very careful about sharing his own PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

83. Plaintiff stores any and all documents containing PII in a secure location, and destroys any documents he receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, he diligently chooses unique usernames and passwords for her various online accounts.

84. Plaintiff suffered actual injury and damages due to LLS's mismanagement of his PII before the Data Breach.

85. Plaintiff suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that he entrusted to LLS for the purpose of providing him mortgage services, which was compromised in and as a result of the Data Breach.

86. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and he has suffered anxiety and increased concerns for the theft of his privacy since he received the Notice Letter. He is especially concerned about the theft of his full name paired with his Social Security number.

87. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

88. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in LLS's possession, is protected and safeguarded from future breaches.

## V. CLASS ALLEGATIONS

89. Plaintiff brings this Action on behalf of herself and on behalf of all other persons similarly situated (the "Class"). Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons who utilized LLS's services, whose Personally Identifiable Information was maintained on LLS's system that was compromised in the Data Breach, and who were sent a notice of the Data Breach (the "Class Definition").

90. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

91. **Numerosity**. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of over 2,300,000 individuals whose sensitive data was compromised in the Data Breach.

92. **Commonality**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether the Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Personally Identifiable Information;

b. 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;

c. Whether Defendant's data security systems prior to, during, and after the Data Breach complied with the applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards, as applicable;

e. Whether Defendant owed a duty to Class Members to safeguard their Personally Identifiable Information;

f. Whether Defendant breached a duty to Class Members to safeguard their Personally Identifiable Information;

g. Whether computer hackers obtained Class Members Personally Identifiable Information in the Data Breach;

h. Whether the Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether the Plaintiff and Class Members suffered legally cognizable injuries as a result of the Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

l. Whether Defendant failed to provide notice of the Data Breach in a timely manner;

m. Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief;

93. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

94. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions.

95. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

96. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

97. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

## VI. CAUSES OF ACTION

### COUNT I

### NEGLIGENCE

98. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in preceding paragraphs.

99. As a condition of receiving their mortgages from partners of Defendant, Defendant's current and former customers were obligated to provide and entrust Defendant with certain PII, including their name, birthdate, address, loan number, Social Security number, and information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

100. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

101. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed or obtained by unauthorized parties.

102. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of its current and former customers' PII involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

103. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and Class Members' information in Defendant's possession was adequately secured and protected.

104. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

105. Defendant had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff and the Class's PII, and to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

106. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship

arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a mandatory step in obtaining services from Defendant.

107. Defendant were subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Class, to maintain adequate data security.

108. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

109. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendant's systems.

110. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's wrongful conduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiff's and the Class's PII, including basic encryption techniques available to Defendant.

111. Plaintiff and the Class had no ability to protect their PII that was in, and remains in, Defendant's possession.

112. Defendant was in a position to effectively protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

113. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to

allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

114. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully accessed by unauthorized third persons as a result of the Data Breach.

115. Defendant, through its actions and inaction, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class when the PII was within Defendant's possession or control.

116. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

117. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its current and former customers' PII in the face of increased risk of theft.

118. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former customers' PII.

119. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove former customers' PII it was no longer required to retain pursuant to regulations.

120. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

121. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

122. There is a close causal connection between (a) Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and (b) the harm or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff and the Class' PII was accessed and exfiltrated as the direct and proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

123. Additionally, 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 of businesses, such as Defendant, of failing to implement reasonable measures to protect PII. The FTC Act and related authorities 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 PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the damages that would result to Plaintiff and the Class.

125. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

126. Plaintiff and the Class are within the class 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 their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

128. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual

identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present 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 other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, 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 current and former customers' PII in its continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

129. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

130. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, 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 PII in its continued possession.

131. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff is now at an increased risk of identity theft or fraud.

132. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff is entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

**COUNT II**

**BREACH OF IMPLIED CONTRACT**

133. Plaintiff and the Class re-alleges and incorporate by reference herein all of the allegations in the preceding paragraphs.

134. Defendant acquired and maintained the PII of Plaintiff and the Class, including name, birthdate, address, loan number, Social Security number, and information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

135. At the time Defendants acquired the PII and PII of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendants would safeguard the PII and not take unjustified risks when storing the PII.

136. Plaintiff and the Class would not have entrusted their PII to Defendants had they known that Defendants would make the PII internet-accessible, not encrypt sensitive data elements such as Social Security numbers, and not delete the PII that Defendants no longer had a reasonable need to maintain.

137. Prior to the Data Breach, Defendant published the Privacy Policy, agreeing to protect and keep private financial information of Plaintiff and the Class.

138. Defendant further promised to comply with industry standards and to ensure that Plaintiff's and Class Members' PII would remain protected.

139. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

140. In collecting and maintaining the PII of Plaintiff and the Class and publishing the Privacy Policy, Defendant entered into contracts with Plaintiff and the Class requiring Defendant to protect and keep secure the PII of Plaintiff and the Class.

141. Plaintiff and the Class fully performed their obligations under the contracts with Defendant.

142. Defendant breached the contracts they made with Plaintiff and the Class by failing to protect and keep private financial information of Plaintiff and the Class, including failing to (i) encrypt or tokenize the sensitive PII of Plaintiff and the Class, (ii) delete such PII that Defendant no longer had reason to maintain, (iii) eliminate the potential accessibility of the PII from the internet where such accessibility was not justified, and (iv) otherwise review and improve the security of the network system that contained such PII.

143. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the

compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; additional time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, credit freezes, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

144. As a direct and proximate result of Defendant's breach of contract, Plaintiff is at an increased risk of identity theft or fraud.

145. As a direct and proximate result of Defendant's breach of contract, Plaintiff is entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

**COUNT III**

**BREACH OF FIDUCIARY DUTY**

146. Plaintiff and the Class re-alleges and incorporate by reference herein all of the allegations contained in the preceding paragraphs.

147. A relationship existed between Plaintiff and the Class and Defendant in which Plaintiff and the Class put their trust in Defendant to protect the private information of Plaintiff and the Class. Defendant accepted that trust and the concomitant obligations.

148. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and not disclose their PII to unauthorized third parties.

149. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

150. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of its current and former customers' PII involved an

unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

151. Defendant's fiduciary duty required it to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff and the Class's information in Defendant's possession was adequately secured and protected.

152. Defendant also had a fiduciary duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and the Class's PII. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant, and because Defendant was the only party in a position to know of its inadequate security measures and capable of taking steps to prevent the Data Breach.

153. Defendant breached the fiduciary duty that it owed to Plaintiff and the Class by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiff and the Class.

154. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiff and the Class.

155. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and the Class would not have occurred.

156. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and the Class.

157. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

## VII. PRAYER FOR RELIEF

158. **WHEREFORE**, Plaintiff, on behalf of themself and all Class Members, request judgment against Defendant and that the Court grant the following:

a. For an Order certifying the Class as defined herein, and appointing Plaintiff and their counsel to represent the Class;

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

c. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personally identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such

information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personally identifying information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining Plaintiff and Class Members' personally identifying information on a cloud-based database;

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

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other areas of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personally identifying information, as well as protecting the personally identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personally identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to adequately educate all Class Members about the threats that they face as a result of the loss of their confidential personally identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and, for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to Class Counsel, and to report any material deficiencies or noncompliance with the Court's final judgment;

d. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

e. For an award of reasonable attorneys' fees, costs, and litigation expenses, as allowed by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this Court may deem just and proper.

## VIII. JURY TRIAL DEMAND

159. Plaintiff hereby demands that this matter be tried before a jury.

DATED: March 31, 2022

Respectfully submitted,

*s/ Jonathan Cohen*

Jonathan Cohen (FL Bar No. 27620)
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**
3833 Central Ave.
St. Petersburg, FL 33713
Tel: 865-247-0080
Email: jcohen@milberg.com

Gary M. Klinger*
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

David K. Lietz*
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
Email: dlietz@milberg.com

Blake Hunter Yagman*
**MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC**
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Tel.: 212-594-5300
Email: byagman@milberg.com

**pro hac vice forthcoming*

*Attorneys for Plaintiff*