UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

EVELYN RIVERA, ALISHIA CARTAGENA, DOREEN ENDRESS, ROBERT KEACH, MAUREEN KEACH, and JAY SAPORTA on behalf of themselves and all others similarly situated, Plaintiffs, vs. LAKEVIEW LOAN SERVICING, LLC, PINGORA LOAN SERVICING, LLC, and BAYVIEW ASSET MANAGEMENT LLC Defendants.	Case No.: **1:22-cv-20968-KMM** **AMENDED CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs Evelyn Rivera, Alishia Cartagena, Doreen Endress, Robert Keach, Maureen Keach, and Jay Saporta ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this Class Action Complaint against Lakeview Loan Servicing, LLC ("Lakeview"), Pingora Loan Servicing, LLC ("Pingora"), and Bayview Asset Management LLC ("Bayview" and collectively with Lakeview and Pingora "Defendants") and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This action stems from Defendants' failure to secure the sensitive personal information of its customers and employees. Defendants Lakeview and Pingora are mortgage loan servicers and Lakeview is the fourth largest mortgage loan servicer in the United States.[1]

2. Lakeview and Pingora are both subsidiaries of Bayview. Bayview also owns

[1] https://lakeview.com (last visited Mar. 30, 2022).

Community Loan Servicing, LLC (formerly known as Bayview Loan Servicing, LLC). Community Loan Servicing, LLC is the fulfillment partner of Lakeview, which means that it provides processing, underwriting and closing functions for loans originated by Lakeview. Bayview provides the privacy notice for Community Loan Servicing, demonstrating its involvement in Lakeview's privacy practices. Lakeview and Pingora obtain certain personally identifying information related to their customers—current and former mortgagees, as well as mortgage applicants—in furtherance of services it performs on their behalf.

3. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard sensitive Personally Identifiable Information provided by and belonging to its customers, including, without limitation, name, address, loan number, and Social Security number and, for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing ("PII").

4. On or around October 27, 2021, an intruder gained entry to Defendants' network system, accessed the PII stored therein, and exfiltrated information from Lakeview and Pingora's systems (the "Data Breach"). In early December 2021, Defendants identified this "security incident involving unauthorized access to [its] file servers."[2] Defendants determined that "an unauthorized person obtained access to files on [its] file storage servers from October 27, 2021 to December 7, 2021."[3]

5. On January 31, 2022, the review process generated a preliminary list of individuals affected by the Data Breach. Defendants determined that the unauthorized actor accessed and exfiltrated the PII of more than 2,537,261 current and former Lakeview customers ("Class Members"), including that of Plaintiffs and Class Members. Defendants also determined that an

[2] Exhibit 1 (sample "Notification Letter" sent to California Attorney General's Office).
[3] *Id.*

unspecified number of Pingora customers were affected, including Plaintiffs Robert Keach, Maureen Keach, Jay Saporta and Class Members.

6. On or around March 18, 2022, Lakeview began notifying Plaintiffs and Class Members of the Data Breach. On or around April 6, 2022, Pingora began notifying Plaintiffs and Class Members of the Data Breach.

7. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties to these individuals. Defendants admit that the unencrypted PII accessed and exfiltrated includes highly sensitive information, such as names, dates of birth, addresses, phone numbers, financial or bank account information, Social Security numbers, insurance information and account numbers, medical information including history, condition, treatment and diagnosis, medical record numbers, driver's license numbers, and email addresses.

8. The exposed PII of Defendants' current and former customers can be sold on the dark web. Plaintiffs are informed and believe that their information has already been placed onto the dark web. Hackers can now access and/or offer for sale the unencrypted, unredacted PII to criminals. Defendants' current and former customers face a lifetime risk of identity theft, which is heightened by the loss of their Social Security numbers.

9. This PII was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect PII of Defendants' current and former customers.

10. Until notified of the breach, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their rest of their lives.

11. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Defendants' current and former customers; (ii) warn Defendants' current and former customers of their inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities. Defendants' conduct amounts to negligence and violates federal and state statutes.

12. Plaintiffs and Class Members have suffered numerous actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damages to and diminution in value of their personal data entrusted to Defendants with the mutual understanding that Defendants would safeguard their PII against theft and not allow access to and misuse of their personal data by others; and (h) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further injurious breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII, and, at the very least, are entitled to nominal damages.

13. Lakeview and Pingora have stated they will protect the privacy of its customers and use security measures to protect its customers' information from unauthorized disclosure.[4]

[4] Exhibit 2 ("Privacy Policy".)

However, Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Lakeview and Pingora's current and former customers' and employee's PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiffs and Class Members was compromised through access to and exfiltration by an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

14. Plaintiffs by this action seek compensatory damages together with injunctive relief to remediate Defendants' failures to secure their and Class Members' PII, and to provide credit monitoring, identity theft insurance, and credit repair services to protect the Class of Data Breach victims from identity theft and fraud.

II. PARTIES

Plaintiff Evelyn Rivera

15. Plaintiff Evelyn Rivera is a resident and citizen the State of Massachusetts and intends to remain domiciled in and a citizen of the State of Massachusetts.

16. Plaintiff Rivera received a letter dated March 16, 2022 from Defendant concerning the Data Breach. The letter stated unauthorized actors gained access to Lakeview Loan Servicing's network containing her name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Alishia Cartagena

17. Plaintiff Alishia Cartagena is a resident and citizen of the State of Massachusetts and intends to remain domiciled in and a citizen of the State of Massachusetts.

18. Plaintiff Cartagena received a letter dated March 16, 2022 from Defendant concerning the Data Breach. The letter stated unauthorized actors gained access to Lakeview Loan Servicing's network containing her name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Doreen Endress

19. Plaintiff Doreen Endress is a citizen and resident of Granby, Connecticut.

20. Plaintiff Endress received a letter dated March 16, 2022 from Defendant concerning the Data Breach. The letter stated unauthorized actors gained access to Lakeview Loan Servicing's network containing her name, address, loan number, Social Security number, and for some, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Robert Keach

21. Plaintiff Robert Keach is a resident and citizen the State of California and intends to remain domiciled in and a citizen of the State of California.

22. Plaintiff Robert Keach received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that his name, address, loan number, and Social Security number were exposed in the Data Breach. The letter also stated that "[f]or some, the accessed files may also have included information provided in connection with a loan application, loan modification, or other items regarding loan servicing."

Plaintiff Maureen Keach

23. Plaintiff Maureen Keach is a resident and citizen the State of California and intends to remain domiciled in and a citizen of the State of California.

24. Plaintiff Maureen Keach received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that her name, address, loan number, and Social Security number were exposed in the Data Breach.

Plaintiff Jay Saporta

25. Plaintiff Jay Saporta is a resident and citizen of the State of California and intends to remain domiciled in and a citizen of the State of California.

26. Plaintiff Jay Saporta received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that his name, address, loan number, and Social Security number were exposed in the Data Breach. The letter also stated that "[f]or some, the accessed files may also have included information provided in connection with a loan application, loan modification, or other items regarding loan servicing."

Defendant Lakeview Loan Servicing, LLC

27. Defendant Lakeview Loan Servicing, LLC is a private mortgage loan servicer organized under the laws of Florida, headquartered at 4425 Ponce de Leon Blvd, Coral Gables, FL 33146, with its principal place of business in Coral Gables, FL.

28. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of Court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

29. All of Plaintiffs' claims stated herein are asserted against Defendant Lakeview and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

Defendant Pingora Loan Servicing, LLC

30. Defendant Pingora Loan Servicing, LLC is a private mortgage loan servicer organized under the laws of Delaware, headquartered at 1819 Wazee Street, 2nd Floor, Denver, CO 80202, with its principal place of business in Denver, Colorado.

31. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of Court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

32. All of Plaintiffs' claims stated herein are asserted against Defendant Pingora and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

Defendant Bayview Asset Management, LLC

33. Defendant Bayview Asset Management, LLC is an investment management services company organized under the laws of Florida, headquartered at 4425 Ponce de Leon Blvd, Coral Gables, FL 33146, with its principal place of business in Coral Gables, FL. Bayview is the parent company of Lakeview and Pingora.

34. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of Court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

35. All of Plaintiffs' claims stated herein are asserted against Defendant Bayview and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns

III. JURISDICTION AND VENUE

36. 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, Plaintiffs, numerous other Class Members, and Defendants are citizens of different states.

37. The Court has general personal jurisdiction over Defendants Lakeview and Bayview because, personally or through its agents, Defendants Lakeview and Bayview 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. Defendants Lakeview and Bayview are also 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.

38. The Court has personal jurisdiction over Defendant Pingora because, personally or through its agents, Defendant Pingora operated, conducted, engaged in, or carried on a business or business venture 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.

39. 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, Defendants Lakeview and Bayview conduct substantial business in this district, and reside in this district. Further, Defendants Lakeview and Bayview are headquartered and does business in and/or has offices for the transaction of its customary business in this district.

IV. FACTUAL ALLEGATIONS

Background

40. Defendant Lakeview is the fourth largest mortgage loan servicer in the United States.[5] Lakeview owns the servicing rights to millions of Americans' mortgage loans. It partners with "several Servicing partners to process payments, manage the escrow, and provide customer service for [more than 1.4 million individuals'] existing mortgage[s]" per year.[6]

41. Bayview—Lakeview's parent company—acquired Pingora Holdings, L.P. and its wholly-owned subsidiary Pingora Loan Servicing, LLC from Annaly Capital Management, Inc. in July 2017 to expand its presence in the mortgage loan industry.

42. Plaintiffs and Class Members who obtained loan services from Lakeview and Pingora were required to entrust some of their most sensitive and confidential information, including, without limitation: name, address, loan number, Social Security number, and additional information provided in connection with a loan application, loan modification, or other items regarding loan servicing. Information that Plaintiffs entrusted to Lakeview and Pinogra is static, does not change, and can be used to commit myriad financial crimes.

43. In providing services to Plaintiffs and Class Members, Lakeview and Pingora generated and retained additional sensitive personal information about Plaintiffs and Class Members, including information concerning their loan services.

44. Plaintiffs and Class Members, as current and former customers of Defendants, relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Defendants' current and former customers demand security to safeguard their PII.

---

[5] https://lakeview.com (last visited Mar. 30, 2022).
[6] *Id.*

45. Defendants had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

46. Defendant Lakeview posts a Privacy Policy on its website.[7] The Privacy Policy states that it collects personal information from its customers, that financial companies "choose how they share your personal information"—though consumers have rights with respect to the sharing of that information—and that Lakeview does not sell consumer information.[8]

47. The Privacy Policy also provides a list of instances in which disclosure of PII could be made to its affiliates and other entities without prior written authorization—none of which is applicable here.[9]

48. Bayview also posts a Privacy Policy on its website.[10] The policy states, "[y]our privacy is very important to us."

49. Bayview's Privacy Policy also states, "The Bayview Funds and the Investment Manager are considered to be data controllers in respect of any personal information we hold about you for the purposes of certain Data Protection Laws. This means that each of the Bayview Funds and the Investment Manager (alone or jointly, as applicable) determines the purposes and the means of the processing of your personal information."[11]

50. On or around October 27, 2021, an intruder gained unauthorized access to Lakeview and Pingora's networks.[12] Defendants discovered the intrusion on or around December

---

[7] Ex. 2.
[8] *See id.*
[9] *See* Ex. 2.
[10] https://bayview.com/privacy-policy/ (last visited April 14, 2022).
[11] *Id.*
[12] Exhibit 3 (sample "Notice of Data Breach" sent to Maine Attorney General's Office); *see also* https://oag.ca.gov/ecrime/databreach/reports/sb24-552339.

7, 2021.[13] Before that discovery, the intruder accessed and exfiltrated the PII of 2,537,261 of current and former Lakeview customers and an unknown number of current and former Pingora customers.[14]

51. On or around March 18, 2022, Lakeview reported the Data Breach to the attorneys general offices of California,[15] Maine,[16] Massachusetts,[17] and Vermont, among other states.[18] On or about that date, it also began notifying Plaintiffs and Class Members of the Data Breach.

52. On or around March 16, 2022, Lakeview sent Plaintiffs and Class members a form "Notice of Data Breach" substantially similar to the sample letters provided to the state Attorneys General.[19]

53. The sample letters slightly varied in length and detail provided. The sample letter to the California Attorney General's Office stated in part:

> Lakeview Loan Servicing, LLC ("Lakeview") understands the importance of protecting the information we maintain. We are writing to inform you of an incident that involved some of your information. This notice explains the incident, measures we have taken, and steps that you may consider taking.
>
> **What Happened?**
>
> Lakeview owns the servicing rights to your mortgage loan. A security incident involving unauthorized access to our file servers was identified in early December 2021. Steps were immediately taken to contain the incident, notify law enforcement, and a forensic

[13] *Id.*
[14] OFFICE OF THE MAINE ATTORNEY GENERAL, Data Breach Notification, *available at* https://apps.web.maine.gov/online/aeviewer/ME/40/3d0c184e-e78c-4123-8ce8-8535f71facd3.shtml (last visited Mar. 30, 2022); *see also* OFFICE OF THE NEW HAMPSHIRE ATTORNEY GENERAL, Data Breach Notification, *available at* https://www.doj.nh.gov/consumer/security-breaches/documents/pingora-loan-servicing-20220406.pdf (last visited Apr. 14, 2022).
[15] Ex. 1.
[16] Ex. 3.
[17] Exhibit 4 (sample "Notice of Data Breach" sent to Massachusetts Attorney General's Office).
[18] Exhibit 5 (sample "Notice of Data Breach" sent to Vermont Attorney General's Office).
[19] *See* Ex. 4.

> investigation firm was engaged. The investigation determined that an unauthorized person obtained access to files on our file storage servers from October 27, 2021 to December 7, 2021. The accessed files were then reviewed by our investigation team to identify the content.
>
> **What Information Was Involved?**
>
> On January 31, 2022, the review process generated a preliminary list of individuals, including you, whose name, address, loan number, and Social Security number were included in the files. We then took extensive measures to review that list to ensure accuracy and prepare the list to be used to mail notification letters. For some, the accessed files may also have included information provided in connection with a loan application, loan modification, or other items regarding loan servicing. The additional loan related information in the files is not the same for all individuals.
>
> **What We Are Doing.**
>
> We regret that this incident occurred and apologize for any inconvenience. Additional steps are being taken to further enhance our existing security measures.[20]

54. Lakeview admitted in the sample letter that unauthorized third persons accessed and removed from its network systems sensitive information about current and former customers of Lakeview, including, without limitation: "name, address, loan number, and Social Security number" and, for some, "information provided in connection with a loan application, loan modification, or other items regarding loan servicing."[21] This sensitive information is static, cannot change, and can be used to commit myriad financial crimes.

55. Pingora began notifying its customers of the Data Breach on April 6, 2022 through letters substantially similar to the Lakeview notification letters.[22]

---

[20] *Id.* at 1.

[21] *Id.*

[22] OFFICE OF THE NEW HAMPSHIRE ATTORNEY GENERAL, Data Breach Notification, *available at* https://www.doj.nh.gov/consumer/security-breaches/documents/pingora-loan-servicing-20220406.pdf (last visited Apr. 14, 2022).

56. Plaintiffs' and Class Members' unencrypted information may have already been leaked onto the dark web, and/or may simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of the affected current and former customers. Unauthorized individuals can access the PII of Defendants' current and former customers now that it has been stolen.

57. Defendants did not use reasonable security procedures and practices suitable or adequate to protect the sensitive, unencrypted information it was maintaining for current and former customers, causing the access and/or exfiltration of the PII of more than 2,537,261 individuals with Lakeview accounts and an unknown number of individuals with Pingora accounts.

Defendants Acquire, Collect and Store Plaintiffs' and Class Members' PII.

58. Defendants acquired, collected, and stored the PII of Lakeview and Pingora's current and former customers.

59. As a condition of doing business with Lakeview and Pingora, Defendants require that their customers entrust them with highly confidential PII.

60. By obtaining, collecting, and storing Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

61. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and the Class Members, as current and former customers, relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

62. Defendants could have prevented this Data Breach by properly securing and

encrypting Plaintiffs' and Class Members' PII. Additionally, Defendants could have destroyed data, including old data that Defendants had no legal right or responsibility to retain.

63. Defendants' negligence in safeguarding Lakeview and Pingora's current and former customers' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data, especially sensitive financial data.

64. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

65. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[23] 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."[24]

66. The ramifications of Defendants' failure to keep secure Lakeview and Pingora's current and former customers' PII are long lasting and severe. Once Social Security numbers and other PII have been stolen, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

67. The PII of individuals is of high value to criminals, as evidenced by the prices they

[23] 17 C.F.R. § 248.201 (2013).

[24] *Id*.

will pay for it on 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.[25] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[26] Criminals also can purchase access to entire sets of information obtained from company data breaches from $900 to $4,500.[27]

68. Social Security numbers are among the most sensitive 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.[28]

69. 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

---

[25] *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 Mar. 30, 2022).

[26] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Mar. 30, 2022).

[27] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Mar. 30, 2022).

[28] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Mar. 30, 2022).

evidence of actual misuse. In other words, preventive action to defend against potential misuse of a Social Security number is not permitted; an individual instead must show evidence of actual, ongoing fraud to obtain a new number.

70. 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."[29]

71. 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, in that situation, 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—name, birthdate, financial history, and Social Security number.

72. This data commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[30]

73. 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.

---

[29] 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 accessed Mar. 30, 2022).

[30] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Mar. 30, 2022).

74. The PII of Plaintiffs and Class Members was taken by hackers to engage in identity theft and/or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[31]

76. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding Lakeview and Pingora's current and former customers' PII, including Social Security numbers and financial account information, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Lakeview and Pingora's current and former customers as a result of such a breach.

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

78. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on their network, comprising millions of individuals' detailed and confidential personal information and, thus, the significant number of individuals who would be

[31] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last visited Mar. 30, 2022).

harmed by the exposure of the unencrypted data.

79. Although Defendants have offered Lakeview and Pingora's current and former customers identity monitoring services for a limited time through Kroll, the offered services are inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

80. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Lakeview and Pingora's current and former customers.

Plaintiff Evelyn Rivera's Experience

81. Plaintiff Rivera used Lakeview Loan Services' services when she took out a mortgage on her home. As a condition to receiving services at Lakeview, upon information and belief, Plaintiff Rivera's PII was provided by her as part of her loan services, which was then entered into Lakeview's database and maintained by Lakeview.

82. Plaintiff Rivera greatly values her privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Rivera took reasonable steps to maintain the confidentiality of her PII.

83. Plaintiff Rivera received a letter dated March 16, 2022 from Defendant concerning the Data Breach.[32] The letter stated that unauthorized actors gained access to Lakeview Loan Servicing's network containing her name, address, loan number, Social Security number, and potentially, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

84. Recognizing the present, immediate, and substantially increased risk of harm

[32] Exhibit 6 (Plaintiff Rivera's "Notice of Data Breach" letter).

Plaintiff Rivera faces, Defendant offered her a two-year subscription to a credit monitoring service. However, Plaintiff Rivera has not signed up for the program, as she has an inherent mistrust of the Lakeview following the Data Breach.

85. In February 2022, Plaintiff Rivera experienced actual identity fraud in the form of an unauthorized $200 charge on her debit card for her checking account. As a result, she was required to obtain a new debit card. She believes the unauthorized $200 charge on her debit card is a result of the Data Breach given that it occurred relatively soon after the Data Breach, and she had no other previous fraudulent charges on her debit card.

86. About a week later, Plaintiff Rivera noticed another $200 charge on her account. She initiated getting a new debit card a second time.

87. Over the course of the first few months of 2022, Plaintiff Rivera had to change her debit card for her bank account three times as she continued to notice $200 charges on her account approximately three times. While she was reimbursed for each unauthorized charge, she lost time in connection with the debit card replacements and her other actions in response to the Data Breach.

88. Since learning of the Data Breach, Plaintiff Rivera has spent additional time reviewing her bank statements and credit cards. Since February 2022, she has spent approximately two hours every day reviewing her bank, credit and debit card statements; procuring a new debit card from her bank—three times; and going to her bank to initiate investigations into the unauthorized charges.

89. Plaintiff also noticed a $360 withdrawal from her CashApp in February 2022. She had to cancel that account and its associated card, and create a new account and request a new card from CashApp. The CashApp was originally linked to the Lakeview bank account. She was

reimbursed for this charge after an investigation concluded that the charge was not actually incurred by her.

90. Plaintiff Rivera has experienced an increase of other spam calls, text messages and emails after the Data Breach.

91. Plaintiff Rivera has received numerous emails showing transactions and invoices using her name and email, for which she is not responsible.

92. The Data Breach has caused Plaintiff Rivera to suffer significant fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

93. Plaintiff Rivera plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

94. Additionally, Plaintiff Rivera is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

95. Plaintiff Rivera stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

96. Plaintiff Rivera has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Alishia Cartagena's Experience

97. Plaintiff Cartagena used Lakeview Loan Services' services when her and her husband's mortgage was sold to Lakeview in 2019. As a condition to receiving services at

Lakeview, upon information and belief, Plaintiff Cartagena's PII was provided by Plaintiff as part of her loan services, after which the PII was entered into Lakeview's database and maintained by it.

98. Plaintiff Cartagena greatly values her privacy and PII, especially when receiving loan and financial services. Prior to the Data Breach, Plaintiff Cartagena took reasonable steps to maintain the confidentiality of her PII.

99. Plaintiff Cartagena received a letter dated March 16, 2022 from Lakeview concerning the Data Breach.[33] The letter stated that unauthorized actors gained access to Lakeview Loan Servicing's network containing her name, address, loan number, Social Security number, and potentially information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

100. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Cartagena faces, Defendant offered Plaintiff Cartagena a two-year subscription to a credit monitoring service. However, Plaintiff Cartagena did not sign up for the program, as she already has credit monitoring through other services.

101. Plaintiff Cartagena has received five notifications through her credit monitoring service that her information was found on the dark web. She first received this notification on February 1, 2022.

102. Since learning of the Data Breach, Plaintiff Cartagena has spent additional time reviewing her bank statements and credit cards. She estimates that she has spent approximately eight hours reviewing her accounts for unauthorized charges since being notified of the Data Breach.

[33] Exhibit 7 (Plaintiff Cartagena's "Notice of Data Breach" letter).

103. She also has experienced an increase in spam phone calls, emails, and text messages since the Data Breach.

104. The Data Breach has caused Plaintiff Cartagena to suffer significant fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

105. Plaintiff Cartagena plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

106. Additionally, Plaintiff Cartagena is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

107. Plaintiff Cartagena stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

108. Plaintiff Cartagena has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Doreen Endress's Experience

109. Plaintiff Endress was a customer with Lakeview at the time of the Data Breach.

110. In late March 2022, Plaintiff Endress received a letter from Lakeview, dated March 16, 2022, informing her of the Data Breach and advising her to take protective measures.

111. After being notified of the Data Breach, Ms. Endress spent time securing financial accounts with additional password protection and two-factor authentication. She also began the process of shopping for a new mortgage servicer, which will require significant expense. Her

sensitive personal information, including her Social Security number, was compromised in the Data Breach. Upon receipt of the Data Breach notification letter, Ms. Endress experienced stress from concerns that she faces an increased risk of identity theft, fraud, and other types of monetary harm.

112. Since learning of the Data Breach, Plaintiff Endress has spent additional time reviewing her bank statements and credit cards.

113. The Data Breach has caused Plaintiff Endress to suffer fear, anxiety, and stress, which has been compounded by the fact that Lakeview has not been forthright with information about the Data Breach.

114. Plaintiff Endress plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her depository, credit, and other accounts for any unauthorized activity.

115. Additionally, Plaintiff Endress is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

116. Plaintiff Endress stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

117. Plaintiff Endress has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Robert Keach

118. Since learning of the Data Breach, Plaintiff Robert Keach made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data

Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and reviewing the credit monitoring offered by Defendant Pingora. Plaintiff Robert Keach has spent several hours dealing with the fallout from the Data Breach, valuable time Plaintiff Robert Keach otherwise would have spent on other activities, including but not limited to work and/or recreation.

119. The Data Breach has caused Plaintiff Robert Keach emotional distress due to the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Robert Keach is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

120. Plaintiff Robert Keach suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff Robert Keach; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

121. As a result of the Data Breach, Plaintiff Robert Keach 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 Robert Keach is at a present, substantial and impending risk and will continue to be at increased risk of identity theft and fraud for years to come.

122. Plaintiff Robert Keach has suffered present and immediate injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third-parties and possibly criminals.

123. Plaintiff Robert Keach has sustained actual damages as a result of the injuries, including the lost value of his PII and emotional distress.

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

Plaintiff Maureen Keach

125. Since learning of the Data Breach, Plaintiff Maureen Keach made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and reviewing the credit monitoring offered by Defendant Pingora. Plaintiff Maureen Keach has spent several hours dealing with the fallout from this Data Breach, valuable time Plaintiff Maureen Keach otherwise would have spent on other activities, including but not limited to work and/or recreation.

126. The Data Breach has caused Plaintiff Maureen Keach emotional distress due to the release of her PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Maureen Keach is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

127. Plaintiff Maureen Keach suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the

value of her PII, a form of property that Defendant obtained from Plaintiff Maureen Keach; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

128. As a result of the Data Breach, Plaintiff Maureen Keach 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 Maureen Keach is at a present, substantial and impending risk and will continue to be at increased risk of identity theft and fraud for years to come.

129. Plaintiff Maureen Keach has suffered present and immediate injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third-parties and possibly criminals.

130. Plaintiff Maureen Keach has sustained actual damages as a result of the injuries, including the lost value of her PII and emotional distress.

131. Plaintiff Maureen Keach has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Jay Saporta

132. Since learning of the Data Breach, Plaintiff Saporta made reasonable efforts to mitigate the impact of the Data Breach—at Defendant's direction—including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; placing a fraud alert on his credit report with all 3 credit report agencies due to the Data Breach, which costs him approximately $15.00 per month; and reviewing the credit monitoring offered by Pingora. Plaintiff Saporta has spent

several hours dealing with the fallout from this Data Breach, valuable time Plaintiff Jay Saporta otherwise would have spent on other activities, including but not limited to work and/or recreation.

133. The Data Breach has caused Plaintiff Saporta emotional distress due to the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Saporta is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

134. Plaintiff Saporta suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff Saporta; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

135. As a result of the Data Breach, Plaintiff Saporta 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 Saporta is at a present, substantial and impending risk and will continue to be at increased risk of identity theft and fraud for years to come.

136. Plaintiff Saporta has suffered present and immediate injury arising from the substantially increased risk of fraud and identity theft resulting from his PII being placed in the hands of unauthorized third-parties and possibly criminals.

137. Plaintiff Saporta has sustained actual damages as a result of the injuries, including the time spent mitigating the likely potential for financial fraud to be perpetrated against him, the lost value of his PII, and emotional distress.

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

V. CLASS ALLEGATIONS

139. Pursuant to Fed. R. Civ. P. 23(a), 23(b)(1), 23(b)(2), 23(b)(3), 23(c)(4) and/or 23(c)(5), Plaintiffs seek to bring this class action on behalf of themselves and a nationwide Class (the "Class") defined as follows.

> All individuals in the United States whose PII was accessed or exfiltrated during the Data Breach of Lakeview Loan Servicing, LLC and Pingora Loan Servicing, LLC in 2021.

140. Plaintiffs Robert Keach, Maureen Keach and Jay Saporta also seek certification of a California sub-class (the "California Subclass") defined as follows:

> All individuals residing in California whose PII was accessed or exfiltrated during the Data Breach of Pingora Loan Servicing, LLC in 2021.

141. The Class and California Subclass are collectively referred to herein as the "Class."

142. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which a Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members and staff.

143. Plaintiffs reserve the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

144. Numerosity. Consistent with Fed. R. Civ. P. 23(a)(1), the Class Members are so numerous that their joinder is impracticable. While the exact number of Class Members is unknown, upon information and belief, it is in excess of two and a half million. The number and identities of Class Members can be ascertained through Defendants' records.

145. Commonality. Consistent with Fed. R. Civ. P. 23(a)(2) and (b)(3), questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;

b. Whether and to what extent Defendants had a duty to protect the PII of Plaintiffs and Class Members;

c. Whether Defendants had duties not to disclose the PII of Plaintiffs and Class Members, respectively, to unauthorized third parties;

d. Whether Defendants had a duty not to use the PII of Plaintiffs and Class Members for non-business purposes;

e. Whether and when Defendants learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants committed violations by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices adequate to protect the information compromised in the Data Breach, considering its nature and scope;

i. Whether Defendants have adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Pingora violated the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*.

k. Whether Defendants engaged in unfair, unlawful, or deceptive practices, including by failing to safeguard the PII of Plaintiffs and Class Members;

l. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct, and if so, in what amount;

m. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct, and if so, in what amount; and

n. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

146. Typicality. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendants' misfeasance, and their claims arise under the same legal doctrines.

147. Policies Generally Applicable to the Class. As provided under Fed. R. Civ. P. 23(b)(2), Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct in relation to the Class and making final injunctive and corresponding declaratory relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly, and Plaintiffs challenge these policies by reference to Defendants' conduct with respect to the Class as a whole.

148. Adequacy of Representation. Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiffs will fairly and adequately represent and protect the interests of the Class Members. No Plaintiff has a disabling conflict of interest with any other Member of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class, and the infringement of rights and the damages they have suffered are typical of other Class Members. Plaintiffs also have retained counsel experienced in complex class action litigation, and they intend to prosecute this action vigorously.

149. Superiority and Manageability. Consistent with Fed. R. Civ. P. 23(b)(3), class treatment is superior to all other available methods for the fair and efficient adjudication of this controversy. Among other things, it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Moreover, class action treatment will permit the adjudication of relatively modest claims by Class Members who could not individually afford to litigate a complex claim against large corporations such as Defendants. Prosecuting the claims pleaded herein as a class action will eliminate the possibility of repetitive litigation. There will be no material difficulty in the management of this action as a class action.

150. Particular issues, such as questions related to Defendants' liability, are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the resolution of such common issues would materially advance the resolution of this matter and the parties' interests therein.

151. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(1), in that the prosecution of separate actions by the 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 Defendants. Prosecution of separate actions by Class Members also would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)
(Against All Defendants)

152. Plaintiffs incorporate and reallege the foregoing allegations of fact.

153. As a condition of receiving their mortgages from partners of Defendants, Lakeview and Pingora's current and former customers were obligated to provide and entrust them 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.

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

155. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed or obtained by unauthorized parties.

156. Defendants knew or reasonably should have known that their 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 Plaintiffs and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

157. Defendants 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 Defendants' security protocols to ensure that Plaintiffs' and Class Members' information in their possession was adequately secured and protected.

158. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII they were no longer required to retain pursuant to regulations.

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

160. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between each Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential PII, a mandatory step in obtaining services from Defendants.

161. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs and the Class, to maintain adequate data security.

162. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

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

164. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and the

Class. Defendants' 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. Defendants' misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiffs' and the Class's PII, including basic encryption techniques available to Defendants.

165. Plaintiffs and the Class had no ability to protect their PII that was in, and remains in, Defendants' possession.

166. Defendants were in a position to effectively protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

167. Defendants had and continue to have a duty to adequately disclose that the PII of Plaintiffs and the Class within Defendants' possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

168. Defendants have admitted that the PII of Plaintiffs and the Class was wrongfully accessed by unauthorized third persons as a result of the Data Breach.

169. Defendants, through their actions and inaction, unlawfully breached their duties to Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Class when the PII was within Defendants' possession or control.

170. Defendants improperly and inadequately safeguarded the PII of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

171. Defendants 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.

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

173. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove former customers' PII they were no longer required to retain pursuant to regulations.

174. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and the Class the existence and scope of the Data Breach.

175. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

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

177. 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 Defendants, of failing to implement reasonable measures to protect PII. The FTC Act and related authorities form part of the basis of Defendants' duty in this regard.

178. Defendants 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.

Defendants' 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 Plaintiffs and the Class.

179. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

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

181. 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 Plaintiffs and the Class.

182. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs 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 Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the current and former customers' PII in their 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 Plaintiffs and the Class Members.

183. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs 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.

184. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

185. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs are now at an increased risk of identity theft or fraud.

186. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)
(Against All Defendants)

187. Plaintiffs incorporate and reallege the foregoing allegations of fact.

188. Defendants acquired and maintained the PII of Plaintiffs 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.

189. At the time Defendants acquired the PII and PII of Plaintiffs 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.

190. Plaintiffs 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.

191. Prior to the Data Breach, Defendants Lakeview and Bayview published a privacy policy, agreeing to protect and keep private financial information of Plaintiffs and the Class.

192. Defendants further promised to comply with industry standards and to ensure that Plaintiffs' and Class Members' PII would remain protected.

193. Implicit in the agreement between Plaintiffs and Class Members and Defendants 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 Plaintiffs 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 Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

194. In collecting and maintaining the PII of Plaintiffs and the Class and publishing the Privacy Policy, Defendants entered into contracts with Plaintiffs and the Class requiring Defendants to protect and keep secure the PII of Plaintiffs and the Class.

195. Plaintiffs and the Class fully performed their obligations under the contracts with Defendants.

196. Defendants breached the contracts they made with Plaintiffs and the Class by failing to protect and keep private financial information of Plaintiffs and the Class, including failing to (i) encrypt or tokenize the sensitive PII of Plaintiffs and the Class, (ii) delete such PII that Defendants 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.

197. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs 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.

198. As a direct and proximate result of Defendants' breach of contract, Plaintiffs are at an increased risk of identity theft or fraud.

199. As a direct and proximate result of Defendants' breach of contract, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)
(Against All Defendants)

200. Plaintiffs incorporate and reallege the foregoing allegations of fact.

201. A relationship existed between Plaintiffs and the Class and Defendants in which Plaintiffs and the Class put their trust in Defendants to protect the private information of Plaintiffs and the Class. Defendants accepted that trust and the concomitant obligations.

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

203. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

204. Defendants 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 Plaintiffs and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

205. Defendants' fiduciary duty required them 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 Defendants' security protocols to ensure that Plaintiffs' and the Class's information in Defendants' possession was adequately secured and protected.

206. Defendants also had a fiduciary duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and the Class's PII. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential PII, a necessary part of obtaining services from

Defendants, and because Defendants were the only parties in a position to know of their inadequate security measures and capable of taking steps to prevent the Data Breach.

207. Defendants breached the fiduciary duty that it owed to Plaintiffs 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 Plaintiffs and the Class.

208. Defendants' breach of fiduciary duty was a legal cause of damage to Plaintiffs and the Class.

209. But for Defendants' breach of fiduciary duty, the damage to Plaintiffs and the Class would not have occurred.

210. Defendants' breach of fiduciary duty contributed substantially to producing the damage to Plaintiffs and the Class.

211. As a direct and proximate result of Defendants' breach of fiduciary duty, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

COUNT IV
Violations of California's Consumer Privacy Act
Cal. Civ. Code § 1798.100, *et seq.* ("CCPA")
(On Behalf of Plaintiffs Robert Keach, Maureen Keach, and Jay Saporta and the California Subclass against Defendant Pingora)

212. Plaintiffs Robert Keach, Maureen Keach, and Jay Saporta incorporate and reallege the foregoing allegations of fact.

213. Defendant Pingora violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiffs' and the California Subclass' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its

duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII.

214. The PII of Plaintiffs and the California Subclass was subjected to unauthorized access and exfiltration, theft, or disclosure as a direct and proximate result of Defendant's violation of its duty under the CCPA.

215. Plaintiffs and the California Subclass lost money or property, including but not limited to the loss of legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as a direct and proximate result of Defendant's acts described above.

216. Defendant knew, or should have known, that its network computer systems and data security practices were inadequate to safeguard PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect PII, such as properly encrypting the PII so in the event of a data breach the PII cannot be read by an unauthorized third party. As a result of the failure to implement reasonable security procedures and practices, the PII of Plaintiffs and members of the California Subclass was exposed.

217. Defendant is organized for the profit or financial benefit of its owners and collects PII as defined in Cal. Civ. Code section 1798.140.

218. Plaintiffs and the California Subclass seek injunctive or other equitable relief to ensure that Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. This relief is important because Defendant still holds PII related to Plaintiffs and the California Subclass. Plaintiffs and the California Subclass have an interest in ensuring that their PII is reasonably protected.

219. On April 14, 2022, Plaintiffs' counsel mailed a CCPA notice letter to Defendants Pingora and Bayview via certified mail. If Defendants do not "actually cure" the effects of the Data Breach, which would require retrieving the PII or securing the PII from continuing and future use, within 30 days of delivery of the CCPA notice letter (which Plaintiffs believes any such cure is not possible under these facts and circumstances), Plaintiffs intend to amend this complaint to seek actual damages, and statutory damages of no less than $100 and up to $750 per customer record subject to the Data Breach, on behalf of the California Subclass as authorized by the CCPA.

PRAYER FOR RELIEF

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

A. For an Order certifying the Class and California Subclass as defined herein, and appointing Plaintiffs and their counsel to represent the Class and California Subclass;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs 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 Plaintiffs and Class Members, including but not limited to an order:

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

ii. requiring Defendants 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 Defendants to delete, destroy, and purge the personally identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

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

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

vi. requiring Defendants 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 Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

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

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

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

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

xi. requiring Defendants 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 Plaintiffs and Class Members;

xii. requiring Defendants 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 Defendants 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 Defendants' policies, programs, and systems for protecting personally identifying information;

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

xv. requiring Defendants 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 Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' 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 Defendants' 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, statutory, consequential, punitive, 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.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: April 14, 2022

Respectfully submitted,

/s/ John A. Yanchunis

JOHN A. YANCHUNIS
RYAN D. MAXEY
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor

Tampa, Florida 33602
Telephone: (813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

Julie Braman Kane
Florida Bar No.: 980277
julie@colson.com
COLSON HICKS EIDSON
255 Alhambra Circle – Penthouse
Coral Gables, Florida 33134
Telephone: (305) 476-7400
Facsimile: (305) 476-7444

Adam E. Polk (*Pro Hac Vice*)
Jordan Elias (*Pro Hac Vice*)
Simon Grille (*Pro Hac Vice*)
Kimberly Macey (*Pro Hac Vice*)
GIRARD SHARP LLP
601 California St, Ste 1400
San Francisco, CA 94108
Telephone: (415) 981-4800
apolk@girardsharp.com
jelias@girardsharp.com
sgrille@girardsharp.com
kmacey@girardsharp.com

Joseph M. Lyon (*Pro Hac Vice Forthcoming*)
THE LYON FIRM, LLC
2754 Erie Avenue
Cincinnati, OH 45208
Telephone: (513) 381-2333
jlyon@thelyonfirm.com

M. ANDERSON BERRY (*pro hac vice* forthcoming)
GREGORY HAROUTUNIAN (*pro hac vice* forthcoming)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com

RACHELE R. BYRD (*pro hac vice* forthcoming)
WOLF HALDENSTEIN ADLER

FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: 619/239-4599
Facsimile: 619/234-4599
byrd@whafh.com

GARY M. KLINGER (*pro hac vice* forthcoming)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

DAVID K. LIETZ (*pro hac vice* forthcoming)
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

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

I HEREBY CERTIFY on April 14, 2022, a true and correct copy of the foregoing has been furnished via email through the Florida Court E-Filing Portal to all counsel of record.

/s/ John A. Yanchunis

JOHN A. YANCHUNIS