

Exhibit A1

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
MIAMI DIVISION**

CASE NO. 1:22-CV-20955-DPG

In re Lakeview Loan Servicing
Data Breach Litigation

DEMAND FOR JURY TRIAL

AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Mark Arthur, Jorge Gonzalez, Robert Keach, Cindy Villanueva, Deborah Hamilton, Michael Kassem, Beth Berg, Savannah Farley, Thomas Lapenter, Hardik Sevak, Peter Wojciechowski, Kimberley Rowton, Jessica Valente-Brodrick, Denise Scott, Nilsa Misencik, David Kraus, John McMahon, Shannon Thomas, Mathew Myers, Jay Saporta, Albert Brumitt, David Cunningham, Linda Kim, Maureen Keach, Pedro Rubio, and Norma Grossman (“Plaintiffs”), individually and on behalf of all others similarly situated, bring this Amended Consolidated Class Action Complaint against Lakeview Loan Servicing, LLC (“Lakeview”), Pingora Loan Servicing, LLC (“Pingora”), Community Loan Servicing, LLC (“Community Loan”), and Bayview Asset Management LLC (“Bayview”) (collectively, “Defendants”), and allege as follows:

I. INTRODUCTION

1. This is a class action arising out of Defendants’ failure to secure the sensitive personal information of consumer borrowers for whom Defendants performed services, resulting in one of the largest data breaches to date in the 2020s.

2. Lakeview, Pingora, and Community Loan are mortgage loan servicers and Bayview

subsidiaries. Lakeview is the fourth largest mortgage loan servicer in the United States.¹

3. Lakeview, Pingora, and Community Loan obtain various personally identifying data of their customers—current and former mortgagors, as well as mortgage applicants—in furtherance of services performed on the customers’ behalf.

4. Each Defendant failed to adhere to industry-standard data security measures, breaching duties owed to the owners of the data. No Defendant adequately protected their current and former customers’ sensitive, personally identifiable information—including names, addresses, dates of birth, Social Security numbers, loan numbers, financial and bank account information, and, for some, additional information provided in connection with a loan application, loan modification, or other items regarding loan servicing (collectively, “PII”).

5. On or around October 25, 2021, an intruder gained entry to Defendants’ linked network systems and then accessed and exfiltrated the PII stored therein (the “Data Breach”). In early December 2021, Bayview, Lakeview, Pingora, and Community Loan identified this “security incident involving unauthorized access to [their] file servers.”² Bayview, Lakeview, Pingora, and Community Loan determined that “an unauthorized person obtained access to files on [their] file storage servers from October 25, 2021 to December 7, 2021.”³

6. Bayview, Lakeview, Pingora, and Community Loan worked together to conduct an internal review process that, by January 31, 2022, generated a preliminary list of individuals affected by the Data Breach. Bayview, Lakeview, Pingora, and Community Loan jointly determined that the unauthorized actor accessed and exfiltrated the PII of at least 2,537,261 current

¹ See Lakeview homepage, Lakeview.com, <https://lakeview.com> (last visited Jan. 12, 2024).

² Exhibit (“Ex.”) 1 (sample “Notification Letters” sent to the California Attorney General’s Office).

³ *Id.*

and former Lakeview customers (including Plaintiffs Jorge Gonzalez, Cindy Villanueva, Deborah Hamilton, Beth Berg, Savannah Farley, Hardik Sevak, Peter Wojciechowski, Jessica Valente-Brodrick, Denise Scott, Nilsa Misencik, John McMahon, Shannon Thomas, Mathew Myers, and Pedro Rubio). Lakeview reported the results of Defendants' investigation to various state attorneys general on March 18, 2022.

7. On June 23, 2022, Lakeview reported that an additional 100,796 Lakeview customers were affected. By November 1, 2022, Bayview, Lakeview, Pingora, and Community Loan had identified a total of 3,920,444 Lakeview customers affected by the Data Breach.

8. Bayview, Lakeview, Pingora, and Community Loan also jointly determined that 1,405,383 Pingora customers were affected by the Data Breach (including Plaintiffs Mark Arthur, Robert Keach, Michael Kassem, Thomas Lapenter, Kimberley Rowton, David Kraus, Jay Saporta, and Maureen Keach), and that 444,534 Community Loan customers were affected (including Plaintiffs Albert Brumitt, David Cunningham, and Linda Kim).

9. All told, at least five million Americans were victims of the Data Breach.⁴ The current and former customers of Lakeview, Pingora, and Community Loan who were victims of the Data Breach are the "Class Members" for purposes of this litigation.

10. On or around March 16, 2022, Lakeview began notifying Plaintiffs and Class Members of the Data Breach. On or around April 6, 2022, Pingora also began notifying Plaintiffs and Class Members. Lakeview issued additional notices beginning in June 2022. On or around May 16, 2022, Community Loan began notifying Plaintiffs and Class Members of the Data Breach.

⁴ Indiana Attorney General Todd Rokita, *Security Breaches*, IN.gov., <https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/security-breaches/#:~:text=The%20Office%20can%20seek%20up,acquired%20by%20the%20wrong%20person> (last visited Jan. 12, 2024).

11. In their notices of the Data Breach, Lakeview, Pingora, and Community Loan recognized that each victim now faces a present and continuing risk of identity theft and fraud, offering Plaintiffs and Class Members limited identity theft protection through Kroll, LLC (“Kroll”), a company that Defendants referred to as a “fraud specialist.” Despite the risk that will remain for the lives of Plaintiffs and Class Members, Defendants only offered identity protection services for one year or, in certain cases, two years. These services offered by Defendants are woefully insufficient to protect Plaintiffs and Class Members from the lifelong ramifications of having their highly confidential PII accessed, acquired, exfiltrated, and/or published on the internet.

12. Lakeview, Pingora, and Community Loan also advised Plaintiffs and Class Members to spend their own time mitigating the fallout from the Data Breach by remaining “vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity.”⁵

13. Defendants’ negligent and careless acts and inaction resulted in an abject failure to protect the PII of Plaintiffs and Class Members. Documents produced in discovery reveal a classic instance of “group think”: individuals responsible for cyber security at each Bayview subsidiary wrongly assumed—but did not verify—that Bayview was taking adequate data security precautions, even as individuals responsible for cyber security at Bayview wrongly assumed—but did not verify—that the subsidiaries were taking adequate data security precautions. In fact, none of the Defendants was taking the necessary, mandatory steps to safeguard and monitor the effectiveness of their electronic security defenses that should have protected Plaintiffs’ and Class Members’ sensitive information.

⁵ Ex. 1.

14. Defendants allowed the deficient security measures and declined to address them despite recognizing they were not doing nearly enough to safeguard consumer PII. Prior to the Data Breach, Bayview acknowledged the [REDACTED] [REDACTED]⁷ When it came to Bayview's electronic security environment, Bayview recognized [REDACTED]⁸ Also prior to the Data Breach, a third-party security vendor [REDACTED] [REDACTED] [REDACTED]⁹ The result of Bayview's inaction, as one Bayview information security executive admitted in the wake of the Data Breach, was [REDACTED] [REDACTED]¹⁰

15. Bayview—the parent company of Lakeview, Pingora, and Community Loan—is ultimately responsible for the data security of the entire enterprise. Bayview's Security Operations Center (the "Bayview SOC") is set up to "protect[] the Bayview brand and assets."¹¹ The Bayview SOC's responsibilities include ensuring: "the monitoring and analysis of incidents to protect People, Technologies and Process addressing all security incidents and ensuring timely escalation"; "daily management, administration & maintenance of security devices to achieve operational effectiveness"; and "threat management, threat modeling, identify threat vectors and

⁶ BAYVIEW000033873-876 at -873; *see also* BAYVIEW000127506-509.

⁷ BAYVIEW000127486.

⁸ BAYVIEW000011422-427 at -422.

⁹ BAYVIEW000002010-011; *see also* BAYVIEW000006898-907 at -900, -906.

¹⁰ BAYVIEW000147612-614 at -612.

¹¹ Security Operations Center Manager at Bayview Asset Management, Salary.com, <https://www.salary.com/job/bayview-asset-management/security-operations-center-manager/j202204210224596678566> (last visited Jan. 12, 2024).

develop use cases for security monitoring.”¹² Analysts within the Bayview SOC are to “perform daily incident response triage communicating accordingly as needed.”¹³ Their duties include “[c]onduct[ing] proactive monitoring, investigation, and mitigation of security incidents” and “[e]nhanc[ing] security operations, analytics, threat hunting, and security orchestration and automation capabilities.”¹⁴

16. Additionally, a “research team” at Bayview relies on engineers to “develop, maintain, and enhance the various databases used to monitor the performance of consumer loans, to improve data pipelines for efficient uploading and downloading of data, to clean the data for use by the research and trading teams, and to help automate reporting data and visualization.”¹⁵ These data analysts also “[i]ntegrate data from multiple sources to meet business requirements.”¹⁶

17. Lakeview, like Bayview, relies on the Bayview research team for data integration and management. Like Bayview, Lakeview invites job applicants to apply for positions on the Bayview research team.¹⁷

18. Lakeview, Pingora, and Community Loan work closely with Bayview on data security matters. The Chief Compliance Officers of Bayview, Lakeview, Pingora, and Community Loan are all [REDACTED]

¹² *Id.*

¹³ Security Operations Center Analyst at Bayview Asset Management, Salary.com, <https://www.salary.com/job/bayview-asset-management/security-operations-center-analyst/j202204210224598508691> (last visited Jan. 12, 2024).

¹⁴ *Id.*

¹⁵ Data Engineer at Bayview Asset Management, DataYoshi.com <https://www.datayoshi.com/offer/388090/data-engineer> (last visited Jan. 12, 2024).

¹⁶ *Id.*

¹⁷ Loan Data Engineer at Lakeview Loan Services, Talentify.com, <https://lakeview-loan-servicing.talentify.io/job/data-engineer-coral-gables-florida-lakeview-loan-servicing-4505?currentPage=3> (last visited July 29, 2022).

¹⁸ The

¹⁹

19. Regardless of whether it was initially collected and/or maintained by Bayview, Lakeview, Pingora, or Community Loan, Plaintiffs’ and Class Members’ confidential PII was among the “Bayview . . . assets”²⁰ that Defendants were obligated—but failed—to protect.

20. By obtaining, collecting, using, and deriving benefits from Plaintiffs’ and Class Members’ PII, each Defendant assumed legal, statutory, and equitable duties to these individuals to safeguard and protect the PII from unauthorized access. Bayview, Lakeview, Pingora, and Community Loan each have admitted that the unencrypted PII accessed and exfiltrated in the Data Breach includes such highly sensitive information as names, dates of birth, addresses, loan numbers, financial or bank account information, and Social Security numbers.²¹

21. The exposed PII of Plaintiffs and Class Members can be and in certain cases has already been sold to other identity thieves or on the dark web—a hidden network of black-market websites that serves as a “haven for all kinds of illicit activity (including the trafficking of stolen

¹⁸ BAYVIEW000147258 at 7261.

¹⁹ BAYVIEW000147258 at 7260-7261.

²⁰ Security Operations Center Manager at Bayview Asset Management, Salary.com, <https://www.salary.com/job/bayview-asset-management/security-operations-center-manager/j202204210224596678566> (last visited Jan. 12, 2024).

²¹ See BAYVIEW000000354; New Hampshire Dep’t of Justice, Office of the Attorney General, *Security Breach Notifications*, <https://www.doj.nh.gov/consumer/security-breaches/> (last visited Jan. 12, 2024); see also Letter from Baker & Hostetler LLP to Attorney General John Formella (Apr. 6, 2022), <https://www.doj.nh.gov/consumer/security-breaches/documents/pingora-loan-servicing-20220406.pdf>.

personal information captured through means such as data breaches or hacks).”²² Plaintiffs John McMahon and Jay Saporta, for example, were informed after the Data Breach that their information has been found on the dark web. Cyber criminals now can indefinitely access, offer for sale, and use the unencrypted, unredacted PII of Plaintiffs and Class Members for nefarious ends. The permanent loss of their Social Security numbers and other PII exposes Plaintiffs and Class Members to an ongoing, lifetime risk of identity theft.

22. Bayview, Lakeview, Pingora, and Community Loan understood the need to protect the privacy of their customers and use security measures to protect their customers’ information from unauthorized disclosure. Bayview, Lakeview, Pingora, and Community Loan further understood the importance of safeguarding PII because they are sophisticated financial entities whose business function is to maintain private and sensitive consumer information. Yet Bayview, Lakeview, Pingora, and Community Loan disregarded the rights of Plaintiffs and Class Members by failing to implement adequate and reasonable measures to ensure that Plaintiffs’ and Class Members’ PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate policies and protocols for the encryption and protection of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised and exfiltrated by an unknown and unauthorized third party.

23. Contrary to industry-standard practices, Bayview improperly failed to encrypt Plaintiffs’ and Class Members’ PII, failed to delete it after it no longer needed to be retained, stored it in a vulnerable, internet-accessible environment, failed to monitor and detect its movement from Bayview’s network to the internet in real time, and failed to monitor or audit the practices of

²² *Ellen Sirull, Paid Content: What is the dark web?* FOX NEWS (Mar. 27, 2018), <https://www.foxnews.com/tech/paid-content-what-is-the-dark-web>.

Bayview's cybersecurity vendors. Nor were these Bayview's only serious lapses: it also improperly failed to include CobaltStrike—the software the attacker used—on the emergency threat feed or to test its “use cases,” thereby allowing the attacker to remain on Bayview's network undetected. And Bayview failed to properly integrate Sentinel One—an all-important threat detection and response tool—into its Security Information and Events Management System. Had Bayview implemented such expected measures, the Data Breach could have been prevented or mitigated.

24. Lakeview, Pingora, and Community Loan each wrongly assumed—but did little, if anything, to verify—that Bayview was ensuring the security of the confidential data in their possession. These mortgage servicer Defendants failed to ensure that Plaintiffs' and Class Members' PII was encrypted, that Bayview deleted the PII after it no longer needed to be retained, or that Bayview monitored and detected movement of the PII from Bayview's network to the internet in real time, while disregarding that Bayview was storing the PII in a vulnerable, internet-accessible environment. These Defendants also failed to monitor or audit the cybersecurity practices of Bayview and its cybersecurity vendors, continued to accept and store PII even after they knew or should have known of the Data Breach, and unreasonably delayed in providing notice of the Data Breach to Plaintiffs and Class Members, who were consequently prevented from taking timely self-protection measures.

25. Until notified of the Data Breach, Plaintiffs and Class Members had no idea that their PII had been compromised and that they were—and will continue indefinitely to be—at significant risk of identity theft and other forms of personal, social, and financial harm.

26. Plaintiffs bring this action on behalf of all persons whose PII was compromised in the Data Breach. Plaintiffs and the Class have suffered actual and present 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 for their respective lifetimes; (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 present 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; (f) damages to and diminution in value of their personal data entrusted to Bayview, Lakeview, Pingora, and Community Loan on the understanding that Bayview, Lakeview, Pingora, and Community Loan would safeguard their PII against theft and prevent access to and misuse of their personal data by others; and (g) the present and continuing risk to their PII, which remains in the possession of Defendants, and which is subject to further injurious breaches, so long as Bayview, Lakeview, Pingora, and Community Loan fail to undertake appropriate and adequate measures to protect the PII. At a minimum, Plaintiffs and Class Members are entitled to damages, identity theft insurance and credit repair services for their respective lifetimes to protect themselves from identity theft and fraud, and injunctive relief tailored to address the vulnerabilities exploited in the Data Breach and to protect their PII from a future breach, together with a Court order directing the destruction of all PII for which Bayview, Lakeview, Pingora, and Community Loan cannot demonstrate a reasonable and legitimate purpose to continue to possess.

II. PARTIES

Plaintiff Mark Arthur

27. Plaintiff Mark Arthur is a resident and citizen of Washington.

28. Plaintiff Arthur received a letter dated November 4, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on

Pingora's network. The compromised files contained his 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.

Plaintiff Jorge Gonzalez

29. Plaintiff Jorge Gonzalez is a resident and citizen of Texas.

30. Plaintiff Gonzalez received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network. The compromised files contained his name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Robert Keach

31. Plaintiff Robert Keach is a resident and citizen of California.

32. Plaintiff Robert Keach received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network. The compromised files contained his name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Cindy Villanueva

33. Plaintiff Cindy Villanueva is a resident and citizen of California.

34. Plaintiff Villanueva received a letter from Defendant Lakeview dated March 17, 2022 concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network. The compromised files contained her name, address, loan number, Social Security number, and may have also included information provided in connection with a loan

application, loan modification, or other items regarding loan servicing.

Plaintiff Deborah Hamilton

35. Plaintiff Deborah Hamilton is a resident and citizen of Georgia.

36. Plaintiff Hamilton received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network. The compromised files contained her name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Michael Kassem

37. Plaintiff Michael Kassem is a resident and citizen of Georgia.

38. Plaintiff Kassem received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network. The compromised files contained his name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Beth Berg

39. Plaintiff Beth Berg is a resident and citizen of Illinois.

40. Plaintiff Berg received a letter dated March 21, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network. The compromised files contained her name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Savannah Farley

41. Plaintiff Farley is a resident and citizen of Indiana.

42. Plaintiff Farley received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network. The compromised files contained her name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Thomas Lapenter

43. Plaintiff Thomas Lapenter is a resident and citizen of New Jersey.

44. Plaintiff Lapenter received a Data Breach notification letter dated April 6, 2022 from Defendant Pingora. The letter stated that unauthorized actors gained access to files on Pingora's network. The compromised files contained his name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Hardik Sevak

45. Plaintiff Hardik Sevak is a resident and citizen of New York.

46. Plaintiff Sevak received a letter dated March 16, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network. The compromised files contained his name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Peter Wojciechowski

47. Plaintiff Peter Wojciechowski is a resident and citizen of Florida.

48. Plaintiff Wojciechowski received a letter from Defendant Lakeview dated March

18, 2022 concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network. The compromised files contained his name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Kimberley Rowton

49. Plaintiff Kimberley Rowton is a resident and citizen of Virginia.

50. Plaintiff Rowton received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network. The compromised files her name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Jessica Valente-Brodrick

51. Plaintiff Jessica Valente-Brodrick is a resident and citizen of Arizona.

52. Plaintiff Jessica Valente-Brodrick's husband received a letter dated March 16, 2022 from Defendant Lakeview concerning the Data Breach, but Defendant did not send her a separate, additional letter. The letter stated that unauthorized actors gained access to files on Lakeview's network. The compromised files contained her husband's name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Denise Scott

53. Plaintiff Denise Scott is a resident and citizen of Florida.

54. Plaintiff Scott received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on

Lakeview's network. The compromised files contained her name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Nilsa Misencik

55. Plaintiff Nilsa Misencik is a resident and citizen of South Carolina.

56. Plaintiff Misencik received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network. The compromised files contained her name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff David Kraus

57. Plaintiff David Kraus is a resident and citizen of Pennsylvania.

58. Plaintiff Kraus received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network. The compromised files contained his name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff John McMahon

59. Plaintiff John McMahon is a resident and citizen of Maryland.

60. Plaintiff McMahon received a letter dated March 16, 2022 from Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network. The compromised files contained his name, address, loan number, Social Security number, and may have also included information provided in connection with a loan

application, loan modification, or other items regarding loan servicing.

Plaintiff Shannon Thomas

61. Plaintiff Shannon Thomas is a resident and citizen of Ohio.

62. On or around March 18, 2022, Plaintiff Thomas received a letter from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network. The compromised files contained her name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Mathew Myers

63. Plaintiff Mathew Myers is a resident and citizen of Texas.

64. Plaintiff Myers received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network. The compromised files contained his name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Jay Saporta

65. Plaintiff Jay Saporta is a resident and citizen of California.

66. Plaintiff Saporta received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network. The compromised files contained his name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Albert Brumitt

67. Plaintiff Albert Brumitt is a resident and citizen of Illinois.

68. Plaintiff Brumitt received a letter dated August 16, 2022 from Defendant Community Loan concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Community Loan's network. The compromised files contained his name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff David Cunningham

69. Plaintiff David Cunningham is a resident and citizen of Illinois.

70. Plaintiff Cunningham received a letter dated October 17, 2022 from Defendant Community Loan concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Community Loan's network. The compromised files contained his name and Social Security number information, and, potentially, information he provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Linda Kim

71. Plaintiff Linda Kim is a resident and citizen of California.

72. Plaintiff Linda Kim received a letter dated October 17, 2022 from Defendant Community Loan concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Community Loan's network. The compromised files contained her name and Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Maureen Keach

73. Plaintiff Maureen Keach is a resident and citizen of California.

74. Plaintiff Maureen Keach received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network. The compromised files contained her name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Pedro Rubio

75. Plaintiff Pedro Rubio is a resident and citizen of California.

76. Plaintiff Pedro Rubio received a letter dated March 17, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network. The compromised files contained his name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Plaintiff Norma Grossman

77. Plaintiff Norma Grossman is a resident and citizen of the State of California.

78. Plaintiff Norma Grossman received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network. The compromised files contained her name, address, loan number, Social Security number, and may have also included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

Defendant Bayview Asset Management, LLC

79. Defendant Bayview Asset Management, LLC is an investment management services company organized under the laws of Florida and headquartered at 4425 Ponce de Leon Blvd., Coral Gables, FL 33146.

80. Bayview is the parent company of Defendants Lakeview, Pingora, and Community Loan and, as such, controls these entities and is responsible for their electronic security and the security of the consumer information maintained by or on behalf of Lakeview, Pingora, and Community Loan.

Defendant Lakeview Loan Servicing, LLC

81. Defendant Lakeview Loan Servicing, LLC is a private mortgage loan servicer 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, Florida.

82. Lakeview is a Delaware limited liability company. It is wholly owned by Bayview MSR Opportunity Corp., an affiliate of Bayview Asset Management, LLC and a Delaware corporation with its principal place of business in Coral Gables, Florida.

Defendant Pingora Loan Servicing, LLC

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

84. Pingora is wholly owned by Bayview Asset Management, LLC.

Defendant Community Loan Servicing, LLC

85. Defendant Community Loan Servicing, LLC is a private mortgage loan servicer organized under the laws of Delaware and headquartered at 4425 Ponce de Leon Blvd., Coral Gables, FL 33146.

86. Community Loan is wholly owned by Bayview Asset Management, LLC.

III. JURISDICTION AND VENUE

87. 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, the minimal diversity requirement is met as Plaintiffs, Class Members, and Defendants are citizens of different states.

88. The Court has personal jurisdiction over Defendants Lakeview, Community Loan, and Bayview because, personally or through their agents, Lakeview, Community Loan, 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, Community Loan, and Bayview are also headquartered in Coral Gables, Florida.

89. The Court has personal jurisdiction over Defendant Pingora because, personally or through its relationship to and the control over it exercised by Bayview, 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.

90. 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, and Defendants Lakeview, Community Loan, and Bayview conduct substantial business in this district and reside in this district. Further, decisions regarding the management of the information security of Plaintiffs' and Class Members' PII were made by

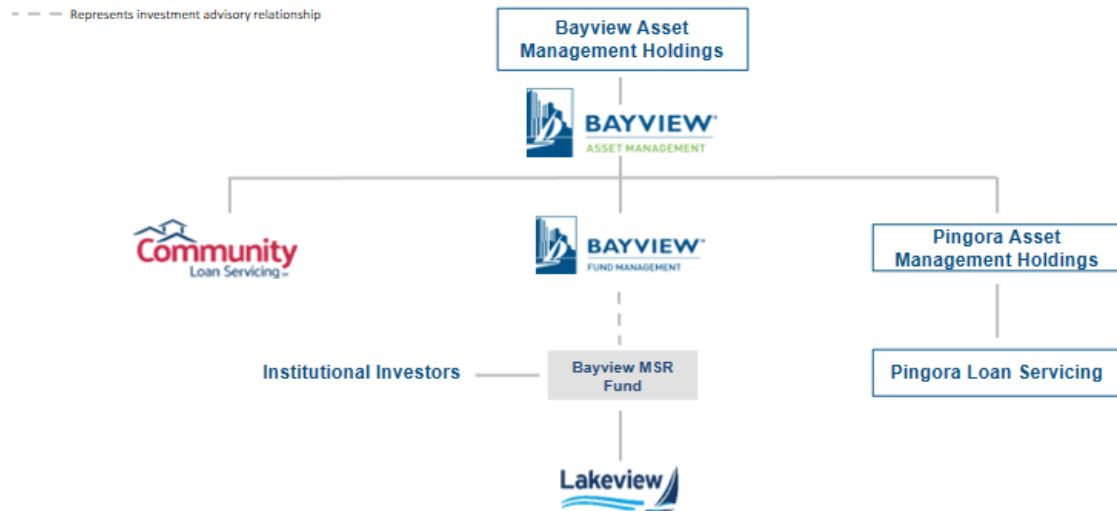
Bayview within this district, Defendants maintain Plaintiffs' and Class Members' PII in this district, and the harm caused to Plaintiffs and Class Members emanated from this district.

IV. FACTUAL ALLEGATIONS

Background on Defendants and Their Corporate Structure and Duties to Protect PII

91. Incorporated in 2008, Bayview is a privately-owned firm that provides discretionary investment management services to private pooled investment vehicles. Bayview focuses on investments in mortgage credit, including whole loans, mortgage-backed securities, mortgage servicing rights, and mortgage-related assets.²³

92. In its corporate policies, "Bayview" or "the Firm" refers to itself as Bayview Asset Management, LLC together with its affiliated group of companies, including Community Loan, Lakeview, and Pingora.²⁴



BAYVIEW000002164.

²³ BAYVIEW000008204-238 at -210.

²⁴ BAYVIEW000002314-327 at -316.

93. Bayview manages asset management-type portfolios, including the Lakeview portfolio.²⁵

94. Lakeview owns the servicing rights to millions of Americans' mortgage loans. It partners with various servicing partners to process payments, manage escrow arrangements, and provide customer service for more than 1.4 million individuals' existing mortgages per year.²⁶

95. In July 2017, Bayview acquired Pingora Holdings, L.P. and its wholly-owned subsidiary, Pingora Loan Servicing, LLC, from Annaly Capital Management, Inc. to expand its presence in the mortgage loan industry.

96. Pingora sources mortgage loan servicing acquisitions for Lakeview.²⁷

97. Community Loan Servicing, LLC, another wholly-owned Bayview subsidiary, maintains a loan servicing platform. For approximately 20 years, Community Loan has provided primary, component, and special mortgage loan servicing for residential and commercial loans owned by Bayview and its affiliates and to certain third parties.²⁸ Bayview "provides primary servicing, third-party component servicing, and special servicing." *Id.*

98. As of autumn 2021, Bayview provided core IT and other services for Lakeview, Pingora, and Community Loan.²⁹

99. Plaintiffs and Class Members received or applied for mortgage-related services from Lakeview, Pingora, or Community Loan, or their mortgage loans or the servicing rights and responsibilities for those loans were acquired by Lakeview, Pingora, or Community Loan. As a

²⁵ Deposition Transcript of Julio Aldecocoea ("Aldecocoea Dep.") 27:4-17 (Mar. 2, 2023).

²⁶ *Id.*

²⁷ Aldecocoea Dep. 25:9-12.

²⁸ BAYVIEW000005825-921 at -832.

²⁹ BAYVIEW000030187; BAYVIEW000002314; Deposition Transcript of Christina Arroyo Maymi ("Arroyo Maymi Dep.") 17:8-14 (June 29, 2023).

result, Plaintiffs were required to entrust some of their most sensitive and confidential information to the care of Defendants in exchange for mortgage services. The information they provided includes names, addresses, loan numbers, Social Security numbers, and additional information provided in connection with a loan application or loan modification, or as necessary for loan servicing. Much of the information Plaintiffs and Class Members entrusted to Lakeview, Pingora, and Community Loan is static, does not change, and can be used to commit myriad financial crimes.

100. In providing services to Plaintiffs and Class Members, Lakeview, Pingora, and Community Loan generated and retained additional sensitive personal information about Plaintiffs and Class Members, including information concerning loan services and information provided to Lakeview, Pingora, and Community Loan by their affiliates and sub-servicers.

101. Sophisticated companies like Defendants are aware of the different types of threat actors operating across the internet and the types of criminal acts that cyber thieves employ for profit. Accordingly, it is imperative that Defendants guard against those criminal exploits.

102. Plaintiffs and Class Members, as current and former customers of Defendants or their affiliates, 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 sensitive information.

103. Defendants had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties. Defendants collected, maintained, and profited from information that they knew to be private and sensitive, and they were aware of the consequences to Plaintiffs and Class Members if they failed to adequately protect that information. Defendants breached their duty to Plaintiffs and Class Members and permitted an attacker to access

Defendants' systems for nearly two months without detection.

Defendants Suffered a Massive Data Breach That Went Undetected for Months

104. On or around October 27, 2021, an intruder gained unauthorized access to Bayview's network.³⁰ Bayview's IT Security team did not discover the intrusion until on or around December 6, 2021.³¹ Before that discovery, the intruder accessed and exfiltrated approximately eight to 20 Terabytes of data, including the PII of 3,920,444 current and former Lakeview customers, 1,405,383 current and former Pingora customers, and 444,534 Community Loan customers.³²

105. The breach stemmed from an incident on [REDACTED], 2021, when a [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]³³

106. On [REDACTED], 2021, [REDACTED]

³⁰ Ex. 3 (sample "Notice of Data Breach" sent to Maine Attorney General's Office); *see also* California Department of Justice, *Submitted Breach Notification Sample*, <https://oag.ca.gov/ecrime/databreach/reports/sb24-552339> (last visited Jan. 12, 2024) (Pingora); California Department of Justice, *Submitted Breach Notification Sample*, <https://oag.ca.gov/ecrime/databreach/reports/sb24-551822> (last visited Jan. 12, 2024) (Lakeview); *see* BAYVIEW000001986.

³¹ *Id.*

³² Office of the Maine Attorney General, *Data Breach Notifications*, <https://apps.web.maine.gov/online/aeviewer/ME/40/3d0c184e-e78c-4123-8ce8-8535f71facd3.shtml> (last visited Jan. 12, 2024) (initially reporting 2,537,261 impacted individuals); Indiana Attorney General Todd Rokita, *Security Breaches*, IN. gov., <https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/security-breaches/#:~:text=The%20Office%20can%20seek%20up,acquired%20by%20the%20wrong%20person> (last visited Jan. 12, 2024).

³³ BAYVIEW000002036.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]³⁶

107. At the time of the Data Breach, [REDACTED]

[REDACTED]³⁷ An [REDACTED]

[REDACTED]

[REDACTED]³⁸ Additionally, one of the [REDACTED]

[REDACTED]

[REDACTED]³⁹ Bayview's failure to include CobaltStrike on the emergency threat

feed, or to test its "use cases," allowed the hacker to remain on Bayview's network undetected.

108. Although [REDACTED]

[REDACTED]⁴⁰ Eventually, Bayview's third-party vendor Compuquip Cybersecurity ("Compuquip") created security alerts on October 25, 2021, and November 8, 2021, which were ultimately addressed on November 10,

³⁴ BAYVIEW000002036-038 at -036.

³⁵ BAYVIEW000007223-233 at -224.

³⁶ BAYVIEW000002036-038 at -036; *see also* BAYVIEW000002158-163 at -160, -163 [REDACTED] BAYVIEW000019979; BAYVIEW000019980.

³⁷ BAYVIEW00002012-020 at -014.

³⁸ *Id.*

³⁹ BAYVIEW000002012 at 2014-15; BAYVIEW000114332.

⁴⁰ BAYVIEW000002036.

2021. Nearly another month went by before the breach was finally mitigated on December 7, 2021.

109. Evidence in this case reveals that, at the time of the Data Breach,

[REDACTED] a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt a business's operations and is an industry-standard data security control.

110. Bayview engaged ReliaQuest, LLC (“ReliaQuest”), a third-party security vendor, to monitor the SIEM, and engaged Compuquip to monitor Sentinel One. At the time of the Data Breach, Bayview had no system in place to consistently communicate findings and patterns between ReliaQuest and Compuquip.

111. On

42

112. That day, Bayview finally began to investigate the Data Breach and

43

113. Bayview then contacted

related to the Data

⁴¹ BAYVIEW000100830-833 at -831.

⁴² BAYVIEW000010129-132 at -132.

⁴³ BAYVIEW000002036-038 at -037.

Breach.⁴⁴

114. On December 9, 2021, Bayview notified [REDACTED]

[REDACTED]⁴⁶

115. During [REDACTED]

[REDACTED]⁴⁷

116. On [REDACTED]

[REDACTED]⁴⁸

117. On or around [REDACTED]

[REDACTED]⁴⁹ After [REDACTED]

[REDACTED]⁵⁰

118. On or around March 18, 2022, Lakeview reported the Data Breach to the Attorneys General offices of California,⁵¹ Maine,⁵² Massachusetts,⁵³ and Vermont, among other states.⁵⁴ On

⁴⁴ Ex. 12 (ECF 136, Ex. B.1).

⁴⁵ BAYVIEW000002012-020 at -014.

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ BAYVIEW000002036-038 at -037; *see also* BAYVIEW000002158-163 (email correspondence with FBI and Secret Service).

⁴⁹ BAYVIEW000019980.

⁵⁰ BAYVIEW000136711-727; BAYVIEW000136728-747.

⁵¹ Ex. 1.

⁵² Ex. 3.

⁵³ Ex. 4 (sample “Notice of Data Breach” sent to Massachusetts Attorney General’s Office).

⁵⁴ Ex. 5 (sample “Notice of Data Breach” sent to Vermont Attorney General’s Office).

or around that date, it also began notifying Plaintiffs and Class Members of the Data Breach.

119. Beginning on or around March 16, 2022, Lakeview sent Plaintiffs and Class Members a form “Notice of Data Breach” substantially similar to the letters sent to the state Attorneys General.⁵⁵ Lakeview sent another round of notices on June 23, 2022 following Lakeview’s discovery of an additional 100,796 victims.

120. Lakeview’s breach notification 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 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

⁵⁵ See Ex. 1.

measures.⁵⁶

121. Lakeview admitted in the sample letter that unauthorized third persons accessed and actually removed PII from its network systems. The exfiltrated PII included information about current and former customers of Lakeview and its affiliates, including, without limitation: “name[s], address[es], loan number[s], and Social Security number[s]” and, for some, “information provided in connection with a loan application, loan modification, or other items regarding loan servicing.”⁵⁷ Much of this PII is static, cannot change, and can be used to commit myriad financial crimes.

122. Pingora began notifying its customers of the Data Breach on April 1, 2022 through letters substantially similar to the Lakeview notification letters.⁵⁸

123. Community Loan began sending such notifications on May 16, 2022.

124. Kroll continued to mail out notifications on behalf of all Defendants through at least October 17, 2022.

125. Plaintiffs’ and Class Members’ unencrypted PII has already been leaked onto the dark web—as evidenced by the dark web notifications received by multiple Plaintiffs and described below. Unauthorized individuals can now access the PII of Plaintiffs and Class Members and use that information to commit fraudulent acts in their names.

126. Defendants did not use reasonable security procedures and practices suitable or adequate to protect the sensitive, unencrypted information they were maintaining for consumers.

⁵⁶ *Id.* at 1.

⁵⁷ *Id.*

⁵⁸ See New Hampshire Dep’t of Justice, Office of the Attorney General, *Security Breach Notifications*, <https://www.doj.nh.gov/consumer/security-breaches/> (last visited Jan. 12, 2024); see also Letter from Baker & Hostetler LLP to Attorney General John Formella (Apr. 6, 2022), <https://www.doj.nh.gov/consumer/security-breaches/documents/pingora-loan-servicing-20220406.pdf>.

Defendants' gross carelessness allowed cybercriminals to access the PII of approximately 5,813,905 individuals.

Defendants Well Understood their Duty to Safeguard the PII in Their Possession

127. All Defendants are sophisticated financial entities that knew or should have known that PII—especially Social Security numbers—is an invaluable commodity and a frequent target of hackers.

128. There were a record 1,802 data breaches in 2022, and 1,862 data breaches in 2021, surpassing 2020's total of 1,108 and the previous record of 1,506 set in 2017.

129. Further, there have been many recent high profile data breaches of 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).

130. Defendants knew or should have known that their electronic records, containing Social Security numbers, among other valuable personal information, would be and/or had been targeted by cybercriminals.

131. Bayview was aware of previous data breaches affecting mortgage providers. In March 2021, Flagstar Bank ("Flagstar") suffered a data breach impacting 1.5 million customers, many of whom were Lakeview's, Pingora's, and Community Loan's borrowers. In [REDACTED]

[REDACTED]

[REDACTED] 59

132. Around the same time, [REDACTED]

⁵⁹ BAYVIEW000127669-673 at -670.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].

133. Cyberattacks have become so prevalent and problematic that the FBI and Secret Service regularly issue warnings to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack. Defendants neglected to do so.

Bayview

134. Bayview knew that the PII it maintained was a target of data thieves and that it had a duty to protect Plaintiffs' and Class Members' PII from unauthorized access.

135. Under its [REDACTED] that:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

136. A [REDACTED]

⁶⁰ BAYVIEW000046204-205 at -204; BAYVIEW000122391-393 at -393.

⁶¹ BAYVIEW000010847-858 at -852

⁶² *Id.*

⁶³ *Id.*

⁶⁴ *Id.*

⁶⁵ *Id.*

[REDACTED]⁶⁶

137. Under its policies and procedures, Bayview implemented network security, with an

[REDACTED]⁶⁷

Lakeview

138. Lakeview knew that the PII it maintained was a target of data thieves and that it had a duty to protect Plaintiffs' and Class Members' PII from unauthorized access.

139. Lakeview posts its Privacy Policy on its website.⁶⁸ This Policy promises consumers that Lakeview will "protect your personal information from unauthorized access and use, [and] use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."⁶⁹ The Privacy Policy further acknowledges that Lakeview collects data directly from consumers when they pay bills, apply for a loan, or provide income or employment information.⁷⁰

140. The Privacy Policy also states that Lakeview will not share its customers' non-public, personal information with affiliates, non-affiliates, and joint marketing partners "unless we first provide you with further privacy choices."⁷¹

141. Lakeview participates in data security meetings organized by Bayview and attended by its affiliates. For example, the [REDACTED]

⁶⁶ BAYVIEW000005066-071 at -071.

⁶⁷ BAYVIEW000002314-327 at -322.

⁶⁸ See Ex. 2.

⁶⁹ *Id.*

⁷⁰ *Id.*

⁷¹ BAYVIEW000006566-574 at 6572.

[REDACTED]

[REDACTED]

[REDACTED]⁷² Lakeview's Chief Compliance Officer is [REDACTED].⁷³

142. Lakeview's Chief Compliance Officer also regularly participates in data security meetings with Bayview officials. [REDACTED]

[REDACTED]

[REDACTED]⁷⁴

[REDACTED]

[REDACTED]⁷⁵

Pingora

143. Pingora knew that the PII it maintained was a target of data thieves and that it had a duty to protect Plaintiffs' and Class Members' PII from unauthorized access.

144. A Pingora [REDACTED]

[REDACTED]

and states that [REDACTED]

[REDACTED]⁷⁶

145. At all relevant times, Pingora has continued to provide a similar "Privacy Notice" to the borrowers whose loans it services.⁷⁷

⁷² BAYVIEW000147258 at 7258, 7260.

⁷³ BAYVIEW000147258 at 7261.

⁷⁴ BAYVIEW000126991 at 6993.

⁷⁵ BAYVIEW000006189-200 at -189.

⁷⁶ BAYVIEW000004233-4332 at -4314.

⁷⁷ *E.g.*, BAYVIEW000003106.

146. Further, Pingora participates in data security meetings organized by Bayview and attended by its affiliates, [REDACTED].⁷⁸ Pingora's Chief Compliance Officer [REDACTED].⁷⁹

147. Pingora's Chief Compliance Officer also regularly participates in data security meetings with Bayview officials. [REDACTED]
[REDACTED].⁸⁰ Pingora's Chief Compliance Officer was [REDACTED].⁸¹

Community Loan

148. Community Loan knew that the PII it maintained was a target of data thieves and that it had a duty to protect Plaintiffs' and Class Members' PII from unauthorized access.

149. Community Loan's Privacy Policy, posted online, states that "[w]e use commercially reasonable security measures to protect the information we have obtained, in accordance with federal and state regulations."⁸²

150. According to the same policy, Community Loan uses "advanced data-encryption and storage technology to protect your sensitive personal information," and "industry-standard encryption to protect data in transit and at rest. Our internal policies and procedures impose a number of standards to safeguard the confidentiality of personal information, prohibit the unlawful disclosure of personal information, and limit access to personal information."⁸³

151. Additionally, Community Loan informs borrowers that, "[t]o protect your personal

⁷⁸ BAYVIEW000147258 at 7260.

⁷⁹ BAYVIEW000147258 at 7261.

⁸⁰ BAYVIEW000126991 at 6993.

⁸¹ BAYVIEW000006189-200 at -189.

⁸² <https://communityloanservicing.com/privacy/> (last accessed Jan. 18, 2024).

⁸³ *Id.*

information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files”⁸⁴

152. Further, Community Loan participates in data security meetings organized by Bayview and attended by its affiliates, including [REDACTED].⁸⁵ Community Loan’s Chief Compliance Officer [REDACTED].⁸⁶

153. Community Loan’s Chief Compliance Officer also regularly participates in data security meetings with Bayview officials. [REDACTED]

[REDACTED]”⁸⁷ Community Loan’s Chief Compliance Officer was [REDACTED]

[REDACTED]⁸⁸

154. Community Loan compliance officers participated in, reviewed, and discussed the results of data security audits conducted by Bayview.⁸⁹

Personal Identifiable Information Commands Substantial Value on the Black Market

155. PII is valuable to criminals, as evidenced by the prices they will pay for it on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information is sold at prices ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.⁹⁰ Experian reports that a stolen credit or debit card number can sell for \$5

⁸⁴ BAYVIEW000171495-97 at -496.

⁸⁵ BAYVIEW000147258 at -7260.

⁸⁶ BAYVIEW000147258 at -7261.

⁸⁷ BAYVIEW000126991 at -6993.

⁸⁸ BAYVIEW000006189-200 at -189.

⁸⁹ BAYVIEW000006189-200 at -190.

⁹⁰ Anita George, *Your Personal Data Is for Sale on the Dark Web. Here’s How Much It Costs*, Digital Trends (Oct. 16, 2019) <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>.

to \$110 on the dark web.⁹¹ Criminals also can purchase access to entire sets of information obtained from company data breaches from \$900 to \$4,500.⁹²

156. Social Security numbers are among the most sensitive kind of personal information that is subject to hacking and theft because they may be put to a variety of fraudulent uses and are extremely 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, when 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.⁹³

157. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against 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.

158. 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

⁹¹ Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017) <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>.

⁹² *In the Dark*, VPNOverview, 2019, <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>.

⁹³ Social Security Administration, *Identity Theft and Your Social Security Number*, July 2021, <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”⁹⁴

159. Thus, 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: names, dates of birth, financial history, and Social Security numbers.

160. This data commands a much higher price on the black market than other PII. Martin Walter, senior director at cybersecurity firm RedSeal, Inc., explained “[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x in price on the black market.”⁹⁵

161. 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. Among other forms of fraud, identity thieves armed with fraudulently obtained Social Security numbers may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

162. The fraudulent activity resulting from the Data Breach may not come to light for years. There also may be a time lag between when harm occurs and when the victim discovers it, as well as between when PII is stolen or sold and when it is misused. According to the U.S.

⁹⁴ Bryan 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-millionsworrying-about-identity-theft>.

⁹⁵ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, NETWORKWORLD (Feb. 6, 2015), <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

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.⁹⁶

163. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding Lakeview’s, Pingora’s, and Community Loan’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 the significant costs that would be imposed on their customers as a result of such a breach.

164. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members 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.

165. Plaintiff and Class Members now face years of needing to continuously monitor their financial and personal records. Plaintiff and Class Members are incurring and will continue to incur such damage, including valuable lost time, in addition to any fraudulent use of their PII, for their respective lifetimes.

166. 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

⁹⁶ United States Government Accountability Office, Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, at 29 (June 2007), <http://www.gao.gov/new.items/d07737.pdf>.

harm by the exposure of the unencrypted data.

167. In recognition of this risk—but failing to address the lifetime exposure to identity theft—Defendants have offered identity monitoring services for only a limited time through Kroll (one year or, for a more limited subset of victims in particular states, two years). The offered services are woefully inadequate to protect Plaintiffs and Class Members from the present and continuing threats they face for years to come, particularly in light of the highly sensitive nature of the stolen PII.

168. 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’s, Pingora’s, and Community Loan’s current and former customers.

Defendants Knew Before the Data Breach That Their Data Security Was Inadequate

169. As a condition of receiving services from Lakeview, Pingora, and Community Loan, Defendants (by way of their affiliate mortgage lenders) require that consumers entrust them with highly confidential PII. Thus, Defendants acquired, collected, and stored the PII of Lakeview’s, Pingora’s, and Community Loan’s current and former customers.

170. By obtaining, collecting, and storing Plaintiffs’ and Class Members’ PII, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs’ and Class Members’ PII from disclosure. Defendants not only breached those duties but their internal documents show that, prior to the Data Breach, they were aware of—yet failed to address—flashing red flags of deficiencies in their electronic security defenses.

171. Despite the prevalence of public announcements of data breach and adverse data security incidents—and their own internal recognition of serious inadequacies in their information security systems—Defendants failed to take appropriate steps to protect the PII of Plaintiffs and

Class Members from being compromised. Defendants could have prevented this Data Breach by properly securing and encrypting Plaintiffs' and Class Members' PII. Defendants also could have limited the harm from the breach by destroying data, including old data that Defendants had no legal right or responsibility to retain.

Bayview

172. Bayview [REDACTED]

[REDACTED]

[REDACTED]”⁹⁷ And yet, as of the date of the Data Breach, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]⁹⁹

173. Bayview knew its security posture was insufficient and failed to timely implement proposed security measures to its environment. For example, Bayview IT employees proposed a network segmentation project in both 2020 and 2021, but Bayview did not undertake the needed segmentation until after the Data Breach. Benefits of network segmentation include securing traffic and providing a [REDACTED]¹⁰⁰

174. Prior to the Data Breach, Bayview knew or should have known that it needed clearer organizational structure and responsibility for maintaining the PII of Defendants'

⁹⁷ BAYVIEW000006189-200 at -190.

⁹⁸ BAYVIEW000002010-011 at -010; *see also* BAYVIEW000006898-907 at -900, -906.

⁹⁹ BAYVIEW000033873-876 at -873 (emphasis added); *see also* BAYVIEW000127506-509

¹⁰⁰ BAYVIEW000038066-070 at -068; *see also* BAYVIEW000048948-949.

customers. Internal documents reveal a classic instance of “group think” and organizational inertia.

In [REDACTED]

”¹⁰¹ [REDACTED]

”¹⁰² [REDACTED]

175. Around the same time, Lakeview, Pingora, and Community Loan staff were participating in their own meetings with Bayview to review data security topics and policies. The agendas for these meetings included items that recognized the urgent need to reform the data security policies and protocols of the enterprise, including: [REDACTED]

[REDACTED]¹⁰³ The meeting agendas also referred to pressing policy goals for Defendants’ data security apparatus, such as [REDACTED]

¹⁰¹ BAYVIEWEW000138037-8038 at -8037.

¹⁰² BAYVIEW000138039-8040 at -8039.

¹⁰³ BAYVIEW000031240-1241 at -1240; BAYVIEW00126859-6860 at -6859; BAYVIEW000126861-6862 at -6861.

[REDACTED] 104

176. Bayview also was keenly aware of inadequacies related to its data security vendors. For example, in an August 17, 2021 email discussing [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] 105

177. Prior to the breach, Bayview employees further conceded that Bayview's privacy protocols [REDACTED] 106

178. Also prior to the breach, Bayview employees [REDACTED]
[REDACTED] 107

179. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] 108

¹⁰⁴ BAYVIEW000031240-1241 at -1240; BAYVIEW00126859-6860 at -6859; BAYVIEW000126861-6862 at -6861.

¹⁰⁵ BAYVIEW000011422-427 at -422 (emphasis added).

¹⁰⁶ BAYVIEW000127486 (emphasis added).

¹⁰⁷ BAYVIEW000138033.

¹⁰⁸ BAYVIEW000148153-180 at -156.

Neither Bayview nor its subsidiaries Lakeview, Pingora, or Community Loan [REDACTED]

[REDACTED] prior to the Data Breach.

180. At the time of the Data Breach, Bayview had [REDACTED]

[REDACTED]. As of October 11, 2021,

Bayview [REDACTED]¹⁰⁹ Similarly deficient, Bayview's information security event logging lacked proper tools to identify potential threats.

181. Likewise, in its December 2021 End of Year Report, distributed to Bayview's Chief Executive Officer and Chief Compliance Officer, Bayview's Chief Information Officer [REDACTED]

182. In Bayview's [REDACTED]

[REDACTED]¹¹² All areas were related to malicious acts,

including the threat of theft of customer data.

183. Just days before the Data Breach, in [REDACTED]

¹⁰⁹ BAYVIEW000100830-833 at -832.

¹¹⁰ BAYVIEW000087865-866 at -865.

¹¹¹ BAYVIEW000008204-238 at -223 (emphasis added).

¹¹² *Id.* at -209.

[REDACTED].¹¹³

184. In [REDACTED]

[REDACTED]

[REDACTED].¹¹⁴ Among [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]¹¹⁶

185. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]¹¹⁸

186. Defendants did not follow [REDACTED].

¹¹³ BAYVIEW000002010-011; *see also* BAYVIEW000006898-907 at -900, -906.

¹¹⁴ BAYVIEW000002578 at slide 3.

¹¹⁵ *Id.*

¹¹⁶ *Id.* at slide 4.

¹¹⁷ *Id.* at slide 7.

¹¹⁸ *Id.* at slide 3.

187. Additionally, [REDACTED]

¹¹⁹ The [REDACTED]

¹²⁰

188. Even after suffering the Data Breach in autumn 2021, Bayview and its affiliates' electronic security policies and protocols remained deficient. In an internal email exchange [REDACTED]

¹²¹

189. [REDACTED]

¹²² A Pingora [REDACTED]

¹²³

190. [REDACTED]

¹²⁴

191. As of September 2022, Bayview's data retention policies remained substandard. In

¹¹⁹ BAYVIEW000088360; *see also* BAYVIEW000006189-200 at -191.

¹²⁰ *Id.* (emphasis added).

¹²¹ BAYVIEW000147612-614 at -612 (emphasis added).

¹²² BAYVIEW000006915 at 6916.

¹²³ BAYVIEW000125645 at 125648-49.

¹²⁴ BAYVIEW000002012-020 at -019-020.

an internal email, [REDACTED]

[REDACTED]

[REDACTED]¹²⁵

192. A year after the Data Breach, Bayview officials still were calling for business segmentation and appropriate PII safeguards. Minutes from [REDACTED]

[REDACTED]

[REDACTED]¹²⁶ For his

part, [REDACTED]

[REDACTED]¹²⁷

193. Thus, even after the Data Breach had demonstrated the inadequacy of Bayview's and its affiliates' data security measures, Defendants still had not made the necessary technical changes, such as periodically deleting PII, limiting access to PII, and clearly delineating areas of responsibility among Bayview and its affiliate entities to avoid confusion over data security.

194. Defendants also failed to comply with basic financial services industry standards for protecting consumer information. For example, prior to the Data Breach, neither Bayview nor its Defendant affiliates had a Chief Information and Security Officer ("CISO"). That role was established by Bayview only after the Data Breach, and there is currently only one CISO—[REDACTED]

[REDACTED]—who oversees data security for Bayview, Lakeview, Pingora, and Community Loan.¹²⁸

195. By failing to take adequate, industry-standard, recommended steps to safeguard its customers' PII, Bayview breached legal and equitable duties owed to Plaintiffs and Class

¹²⁵ BAYVIEW000100276-277 at -276.

¹²⁶ BAYVIEW000006915-16 at -16

¹²⁷ *Id.* (emphasis added).

¹²⁸ Deposition Transcript of [REDACTED] ("[REDACTED].") 14:16-22, 15:6-9, 124:3-8 (Mar. 2, 2023).

Members.

Lakeview

196. Lakeview acquired, collected, and stored the PII of its prior and current customers as a precondition for providing services related to their mortgages.

197. Lakeview used the Bayview network to upload and store the PII of its customers. Although Bayview managed the network, Lakeview made decisions as to what data was saved, where it was saved, for how long it was saved, and which individuals had permission to access it.

198. Despite having this level of control over its customers PII, Lakeview did not periodically delete PII for which it no longer had a legitimate business interest in retaining; nor did it instruct Bayview to do so.¹²⁹

199. In [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

¹³⁰

200. Lakeview did not encrypt the PII it stored on Bayview's network, and knew or should have known that such PII was not encrypted.¹³¹ Bayview's IT department decided what encryption software to use, but Lakeview itself determined which data on its system needed to be encrypted. Lakeview's flagrant failure to encrypt its customers' Social Security numbers and other highly confidential PII exposed this information to unnecessary risk and allowed hackers to obtain it.

201. Even after Lakeview knew or should have known about the Data Breach, it

¹²⁹ BAYVIEW000100276-277 at -276; BAYVIEW000147612-614 at -612.

¹³⁰ BAYVIEW000006915 at 6916.

¹³¹ BAYVIEW000002010-011 at -010.

continued to maintain unencrypted PII of its customers on its servers instead of deleting it.¹³²

Community Loan

202. Community Loan acquired, collected, and stored the PII of its prior and current customers as a precondition for providing services related to their mortgages.

203. Community Loan used the Bayview network to upload and store the PII of its customers. Although Bayview managed the network, Community Loan made decisions as to what data was saved, where it was saved, for how long it was saved, and which individuals had permission to access it.

204. Despite having this level of control over its customers PII, Community Loan did not periodically delete PII for which it no longer had a legitimate business interest in retaining; nor did it instruct Bayview to do so.¹³³

205. Community Loan did not encrypt the PII it stored on Bayview's network, and knew or should have known that such PII was not encrypted.¹³⁴ Bayview's IT department decided what encryption software to use, but Community Loan itself determined which data on its system needed to be encrypted. Community Loan's flagrant failure to encrypt its customers' PII exposed their information to unnecessary risk and allowed hackers to exfiltrate their data.

206. Even after Community Loan knew or should have known about the Data Breach, it continued to maintain its customers' unencrypted PII on its servers instead of deleting it.¹³⁵

¹³² BAYVIEW000100276-277 at -276; BAYVIEW000147612-614 at -612.

¹³³ BAYVIEW000100276-277 at -276; BAYVIEW000147612-614 at -612.

¹³⁴ BAYVIEW000002010-011 at -010.

¹³⁵ BAYVIEW000100276-277 at -276; BAYVIEW000147612-614 at -612.

Pingora

207. Pingora acquired, collected, and stored the PII of its prior and current customers as a precondition for providing services related to their mortgages.

208. Pingora used the Bayview network to upload and store the PII of its customers. Although Bayview managed the network, Pingora made decisions as to what data was saved, where it was saved, for how long it was saved, and which individuals had permission to access it.

209. Despite having this level of control over its customers PII, Pingora did not periodically delete PII for which it no longer had a legitimate business interest in retaining; nor did it instruct Bayview to do so.¹³⁶

210. Pingora knew or should have known that it had no business interest in retaining its customers PII, and that maintaining it without encryption posed a dire security risk. For example,

a [REDACTED]

[REDACTED] Pingora's

[REDACTED]

[REDACTED]

[REDACTED]¹³⁷ The [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] ¹³⁸

211. Mortgage servicers transmit files to Pingora on a daily basis which are ingested into Pingora's databases. Pingora acknowledged that [REDACTED]

¹³⁶ BAYVIEW000100276-277 at -276; BAYVIEW000147612-614 at -612.

¹³⁷ BAYVIEW000125645 at 125648-49.

¹³⁸ *Id.*

[REDACTED]

[REDACTED]¹³⁹

212. Pingora did not encrypt the PII it stored on Bayview’s network, and knew or should have known that such PII was not encrypted.¹⁴⁰ Bayview IT decided what encryption software to use, but Pingora determined which data on its system needed to be encrypted. Pingora’s flagrant failure to encrypt its customers’ PII exposed their information to unnecessary risk and allowed hackers to exfiltrate their data.

213. Even after Pingora knew or should have known about the Data Breach, it continued to maintain its customers’ unencrypted PII on its servers instead of deleting it.¹⁴¹

Defendants’ Inadequate Data Security Measures Failed to Comply with Regulations and Industry Practices

214. Defendants’ inadequate security measures violated applicable rules, regulations, and standards regarding data security. By not taking adequate security measures, Defendants Bayview, Lakeview, Pingora, and Community Loan violated the Gramm-Leach-Bliley Act (“GLBA”), 15 U.S.C. § 6801, *et seq.*, and the industry best practices that the GLBA requires for financial institutions.

215. The GLBA defines a financial institution as “any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956].” 15 U.S.C. § 6809(3)(A). Defendants qualify as financial institutions under this definition and hence are subject to the GLBA.

216. Defendants collect nonpublic PII, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R.

¹³⁹ *Id.*

¹⁴⁰ BAYVIEW000002010-011 at -010.

¹⁴¹ BAYVIEW000100276-277 at -276; BAYVIEW000147612-614 at -612.

§ 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant period Defendants were subject to the requirements of the GLBA, 15 U.S.C. § 6801.1, *et seq.*, and are subject to numerous rules and regulations promulgated under the GLBA.

217. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 (“Regulation P”), with the final version taking effect on October 28, 2014.

218. Accordingly, Defendants’ conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

219. Further, the Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards’ key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and

monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Defendants violated the Safeguard Rule.

220. Defendants failed to assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information.

221. Defendants' conduct resulted in myriad failures to follow GLBA-mandated rules and regulations, many of which are also industry standard. Among such deficient practices, the Defendants failed to implement (or inadequately implemented) information security policies or procedures such as effective employee training, sufficient endpoint threat detection and response systems, regular reviews of audit logs and records, proper encryption and storage of customers' PII, and other similar measures to protect the confidentiality of the PII Defendants maintained in their data systems.

222. Defendants' security failures also demonstrate that they failed to honor their express and implied promises, including by failing to:

- a. maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;
- b. adequately protect borrowers' PII from unauthorized disclosure;
- c. implement policies and procedures to prevent, detect, contain, and correct security violations;
- d. implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports;
- e. protect against any reasonably anticipated threats or hazards to the security or integrity of PII; and
- f. effectively train all members of their workforce on the policies and procedures

with respect to PII as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of PII.

223. Had Defendants implemented such data security protocols, the consequences of the Data Breach could have been avoided, or at least significantly reduced (inasmuch as the exposure could have been detected earlier); the amount of PII compromised could have been greatly reduced; and affected consumers could have been notified—and taken self-protection and mitigating actions—much sooner.

224. Defendants' practices also violated the FTC Act, 15 U.S.C. § 45. The FTC has brought enforcement actions under the FTC Act against businesses for failing to adequately and reasonably protect customer 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 Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

225. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data. Similarly, the body of law created by the FTC and generated by its enforcement actions recognizes that failure to restrict access to information and failure to segregate access to information may violate the FTC Act.

226. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

V. PLAINTIFF-SPECIFIC ALLEGATIONS

Plaintiff Mark Arthur's Experience

227. Plaintiff Mark Arthur did not use Pingora's services when he took out a mortgage

on his home. To his knowledge, Pingora has never serviced his mortgage and he has never willingly provided any of his PII to Pingora. Instead, as a condition to receiving loan services from his mortgage originator and servicers, whom he believes provided his PII to Pingora, Plaintiff Arthur provided his PII to those mortgage originators and servicers, which they provided to Pingora. The PII was then entered into Pingora's database and maintained by Pingora on Bayview's network.

228. Plaintiff Arthur greatly values his privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Arthur took reasonable steps to maintain the confidentiality of his PII.

229. Plaintiff Arthur received a letter dated November 4, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network that contained his 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.

230. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Arthur faces, Defendant Pingora offered him a one-year subscription to a credit monitoring service. Plaintiff Arthur has not signed up for the program as he does not trust Defendant's chosen vendor with his PII. Additionally, Plaintiff Arthur does not believe this is sufficient to protect his identity from the ongoing risks of theft he faces.

231. Since learning of the Data Breach, Plaintiff Arthur has spent additional time reviewing his bank statements, credit cards, and reviewing his emails for fraud alerts. Since November 2022, he has spent approximately five hours reviewing his bank, credit and debit card statements; and reviewing his emails for fraud alerts or otherwise suspicious account activity.

Moreover, Plaintiff expended this time at Pingora's direction. In the notice letter Plaintiff received, Pingora directed Plaintiff to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

232. Plaintiff Arthur has experienced an increase of other spam calls, text messages, and emails after the Data Breach, receiving new spam emails daily.

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

234. Additionally, Plaintiff Arthur is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

235. Plaintiff Arthur stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently and periodically chooses unique usernames and passwords for his various online accounts.

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

Plaintiff Jorge Gonzalez's Experience

237. Plaintiff Gonzalez used Lakeview's services when his home mortgage was transferred to Lakeview. As a condition to receiving loan services from Lakeview, Plaintiff Gonzalez provided Lakeview with his PII, which was then entered into Lakeview's database and maintained by Lakeview on Bayview's network.

238. Plaintiff Gonzalez greatly values his privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Gonzalez took reasonable

steps to maintain the confidentiality of his PII.

239. Plaintiff Gonzalez received a letter dated March 18, 2022, from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained his 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.

240. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Gonzalez faces, Defendant Lakeview offered him a one-year subscription to a credit monitoring service. Plaintiff Gonzalez signed up for the program on April 6, 2022, in an attempt to mitigate the harms he suffered as a result of the Data Breach. Plaintiff Gonzalez froze his credit and opened an account with the FTC to report fraud and obtain a Recovery Plan from Identity Theft the day after he received the Notice of Data Breach. Plaintiff Gonzalez changed his passwords and contacted his bank. Plaintiff Gonzalez has also purchased Experian credit monitoring at a cost of \$34.99 per month, and Zandar Insurance at a cost of \$145 per year.

241. Since the Data Breach, Plaintiff Gonzalez experienced identity fraud in the form of fraudulent financial accounts opened using his information. For example, on or around April 11, 2022, Plaintiff Gonzalez received a Chime Visa Debit card that he had not applied for. Similarly, in April 2022, Plaintiff Gonzalez received notice of a Wells Fargo account that had fraudulently been opened around March 26, 2022, using his PII. On or around July 14, 2022, Plaintiff Gonzalez received an email notification welcoming him to a checking account that he had not opened. On or around August 13, 2022, Plaintiff Gonzalez received a notification from his Experian credit monitoring service, which advised him that his Social Security number had been used to open a Defendants 360 account.

242. As a result of the opening of these unauthorized accounts, Plaintiff Gonzalez was required to contact the respective institutions to immediately close each of the accounts. Plaintiff Gonzalez also filed police reports about these fraudulent accounts. He reasonably believes the unauthorized accounts were opened as a result of the Data Breach given that these incidents occurred relatively soon after the Data Breach, and he had experienced no other previous incidents like this.

243. Plaintiff Gonzalez has had to close three unauthorized financial accounts that were fraudulently opened using his PII. He spent considerable time in connection with closing these accounts, filing police reports, contacting the Social Security office and USAA Bank Services about the Data Breach and the subsequent identity theft, contacting the FTC and opening an account with identitytheft.gov, freezing his credit reports, and taking other actions in response to the Data Breach. Since learning of the Data Breach, Plaintiff Gonzalez has spent additional time reviewing his bank statements, credit cards, and credit monitoring reports.

244. Plaintiff Gonzalez estimates that he spent approximately 15 hours on the foregoing mitigation steps. Plaintiff expended this time at Lakeview's direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

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

246. Plaintiff Gonzalez also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant Lakeview in exchange for mortgage services.

247. Plaintiff Gonzalez has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially with his Social Security number now in the hands of criminals.

248. Because of the Data Breach, Plaintiff Gonzalez is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

249. Additionally, Plaintiff Gonzalez is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

250. Plaintiff Gonzalez stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently and periodically chooses unique usernames and passwords for his various online accounts.

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

Plaintiff Robert Keach's Experience

252. As a condition to receiving loan services from his mortgage originator and servicers, whom he believes provided his PII to Pingora, Plaintiff Keach provided his PII to those mortgage originators and servicers. The PII was then provided to Pingora and entered into Pingora's database and maintained by Pingora on Bayview's network.

253. Plaintiff Keach greatly values his privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Keach took reasonable steps to maintain the confidentiality of his PII.

254. Plaintiff Keach received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on

Pingora's network that contained his 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.

255. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Keach faces, Defendant Pingora offered him a one-year subscription to a credit monitoring service. Plaintiff Keach has signed up for the program but does not believe it is sufficient to protect his identity from the ongoing risks of theft he faces into the indefinite future. Plaintiff also signed up for McAfee and Avast around April 6, 2022.

256. In December 2021, Plaintiff Keach experienced identity fraud in the form of an unauthorized \$413 charge for a "security plan" through "Geek Squad"; and in April 2022 he had an unauthorized charge of \$284.99 from Norton LifeLock. He believes these unauthorized charges are a result of the Data Breach given that they occurred after the Data Breach, and he had experienced no previous fraudulent charges.

257. Since learning of the Data Breach, Plaintiff Keach has spent additional time reviewing his bank statements, credit cards, and reviewing his emails for fraud alerts. Since April 2022, he has spent approximately one hour every day reviewing his bank, credit and debit card statements; and reviewing his emails for fraud alerts or otherwise suspicious account activity. Plaintiff expended this time at Pingora's direction. In the notice letter Plaintiff received, Pingora directed Plaintiff to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

258. Plaintiff Keach has experienced an increase in spam calls, text messages and emails since the Data Breach.

259. Plaintiff Keach has received numerous emails showing transactions and invoices

using his name and email, for which he is not responsible.

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

261. Plaintiff Keach also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant Pingora in exchange for mortgage services.

262. Plaintiff Keach has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially with his Social Security number now in the hands of criminals.

263. Because of the Data Breach, Plaintiff Keach is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

264. Additionally, Plaintiff Keach is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

265. Plaintiff Keach stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently and periodically chooses unique usernames and passwords for his various online accounts.

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

267. Pursuant to § 1798.150(b) of the CCPA, Plaintiff Keach gave written notice to Defendant Pingora and Bayview of their specific violations of § 1798.150(a) by certified mail

dated April 14, 2022.¹⁴² Pingora responded on April 29, 2022 but failed to cure.¹⁴³ Bayview has not responded.

Plaintiff Cindy Villanueva's Experience

268. Plaintiff Villanueva took out a loan to purchase her home. The original servicer was Dignified Home Loans. On or around December 6, 2019, Lakeview purchased the mortgage. As a condition to providing Plaintiff Villanueva loan services, Lakeview required access to Plaintiff Villanueva's PII, which it received and entered into its database on Bayview's network to maintain.

269. Plaintiff Villanueva greatly values her privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Villanueva took reasonable steps to maintain the confidentiality of her PII.

270. Plaintiff Villanueva received a letter dated March 17, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained 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.

271. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Villanueva faces, Defendant Lakeview offered her a one-year subscription to a credit monitoring service.

272. In or around April 2022, Plaintiff Villanueva discovered that an individual in Washington was attempting to purchase approximately \$900 worth of electronics using her

¹⁴² Ex. 6 (R. Keach, M. Keach, and Saporta CCPA Notice).

¹⁴³ Ex. 7 (CCPA Responses).

Amazon account. Later the same month, Plaintiff Villanueva was notified that a second subscription to Amazon was opened in her name and her account was charged \$150.

273. Later the same month, Plaintiff Villanueva received a call from a man purporting to be an Amazon employee, who claimed that someone had tried to purchase a phone with her Amazon account, and tried to convince her to open two Bitcoin accounts. Later that day, Plaintiff Villanueva received alerts from her bank that someone had attempted to open two new accounts in her name, requiring her to call her bank and later drive to the bank location in person.

274. Plaintiff Villanueva has also experienced various unauthorized deductions continuously appearing in her checking account. Plaintiff Villanueva cancelled her debit card and requested a new one to stop the unauthorized charges.

275. Plaintiff Villanueva spent considerable time addressing the unauthorized Amazon account and debit card charges.

276. Since learning of the Data Breach, Plaintiff Villanueva has spent additional time reviewing her bank statements and credit cards. Every day, she reviews her Amazon account information and bank, credit card and debit card statements. She often has to go to her bank to dispute unauthorized charges. Plaintiff Villanueva expended this time at Lakeview's direction. In the notice letter Plaintiff Villanueva received, Lakeview directed Plaintiff Villanueva to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

277. Plaintiff Villanueva has experienced an increase in spam calls, text messages, and emails after the Data Breach. As a result of this increase in spam, Plaintiff Villanueva stopped using her Hotmail email address.

278. Plaintiff Villanueva plans to take 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.

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

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

281. Plaintiff Villanueva 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.

282. On April 29, 2022 Plaintiff Villanueva transmitted a 30-day Notice of Claim pursuant to Cal. Civ. Code § 1798.150 to Defendant Lakeview alleging it violated the CCPA and demanding it cure such violation within 30 calendar days of the date of her Notice of Claim.

283. Lakeview never responded to Plaintiff Villanueva's Notice of Claim.

Plaintiff Deborah Hamilton's Experience

284. Plaintiff Hamilton took out a loan to purchase her home. The original servicer was Fairway Independent Mortgage. Lakeview purchased the mortgage. As a condition to providing Plaintiff Hamilton loan services, Lakeview required access to Plaintiff Hamilton's PII, which it received and entered into its database on Bayview's network to maintain.

285. Plaintiff Hamilton greatly values her privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Hamilton took reasonable steps to maintain the confidentiality of her PII.

286. Plaintiff Hamilton received a letter dated March 18, 2022, from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained 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.

287. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Hamilton faces, Defendant Lakeview offered her a one-year subscription to a credit monitoring service. Plaintiff Hamilton signed up for the program in an attempt to mitigate the harms she suffered as a result of the Data Breach. She also purchased LifeLock identity theft protection at an annual cost of \$339 per year on or around July 25, 2022. On or around July 2023, Plaintiff Hamilton renewed LifeLock at an additional fee of \$349 because the monitoring service, Kroll, provided by Lakeview only lasted for one year.

288. On or around February 23, 2022, Plaintiff Hamilton experienced identity fraud in the form of an unauthorized charge of \$508 on her payment card. As a result, she was required to file a police report in response to the fraudulent charge. She believes the unauthorized charge 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 card.

289. Since learning of the Data Breach, Plaintiff Hamilton has spent additional time reviewing her bank statements and credit card statements. Plaintiff Hamilton estimates she has spent approximately 10 hours per month responding to the Data Breach, including: reviewing her bank, credit, and debit card statements; attempting to obtain reimbursement of the \$508 unauthorized charge; filing a police report about the fraudulent charge; and calling Lakeview to confirm the Data Breach and obtain further information. Plaintiff expended this time at Lakeview's

direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating her losses by “reviewing your account statements and free credit reports for unauthorized activity.”

290. Plaintiff Hamilton 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.

291. Plaintiff Hamilton also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant Lakeview in exchange for mortgage services.

292. Plaintiff Hamilton has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially with her Social Security number now in the hands of criminals.

293. Because of the Data Breach, Plaintiff Hamilton is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

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

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

296. Plaintiff Hamilton 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 Michael Kassem's Experience

297. Plaintiff Kassem used Pingora's services when his home mortgage was transferred to Pingora. As a condition to receiving loan services from Pingora, Plaintiff Kassem's PII was provided to Pingora, which was then entered into Pingora's database and maintained by Pingora on Bayview's network.

298. Plaintiff Kassem greatly values his privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Kassem took reasonable steps to maintain the confidentiality of his PII.

299. Plaintiff Kassem received a letter dated April 6, 2022, from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network that contained his 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.

300. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Kassem faces, Defendant Pingora offered him a one-year subscription to a credit monitoring service. Plaintiff Kassem signed up for the program in an attempt to mitigate the harms he suffered as a result of the Data Breach. Plaintiff Kassem has also purchased Experian credit monitoring at a cost of \$25 per month because he does not believe the program offered by Pingora is sufficient.

301. Since the Data Breach, Plaintiff Kassem experienced identity fraud in the form of unemployment fraud. In or around December 2021, Plaintiff Kassem was notified by the Georgia Department of Labor that someone had filed a fraudulent unemployment claim using his Social Security number. As a result, he was required to contact the Department of Labor concerning the

fraudulent unemployment claim. He also filed a police report concerning the incident. Plaintiff Kassem had to drive to the police station to file the police report concerning fraudulent unemployment claim and estimates that he expended approximately \$12 in gas money as a result. Plaintiff Kassem believes the fraudulent unemployment claim is a result of the Data Breach given that it occurred relatively soon after the Data Breach, and he has had no previous experiences of fraudulent unemployment claims being filed using his PII.

302. On June 20, 2022, Plaintiff Kassem's PayPal account was used without authorization. On September 24, 2022, Plaintiff Kassem's Regions bank account was accessed without authorization. On June 19, 2022, and September 10, 2022, his Truist bank account was accessed without authorization. On September 9, 2022, his Wells Fargo bank account was accessed without authorization. Plaintiff believes these unauthorized actions are a result of the Data Breach due to the proximity in time.

303. Plaintiff Kassem locked his accounts with Equifax, Transunion and Experian on September 6, 2022.

304. Plaintiff Kassem spent considerable time in connection with reporting the fraudulent unemployment claim and coordinating with the Department of Labor about the issue; filing a police report; researching and signing up for credit monitoring; placing a freeze on his credit reports; reviewing his bank statements, credit card statements, and credit monitoring reports; carefully reviewing his emails and other personal information for suspicious activity; and taking other steps in an attempt to mitigate the harm caused as a result of the Data Breach.

305. Plaintiff Kassem estimates that he has spent more than 40 hours on the foregoing mitigation steps. Plaintiff expended this time at Pingora's direction. In the notice letter Plaintiff received, Pingora directed Plaintiff to spend time mitigating his losses by "reviewing your account

statements and free credit reports for unauthorized activity.”

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

307. Plaintiff Kassem also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant Pingora in exchange for mortgage services.

308. Plaintiff Kassem has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially with his Social Security number now in the hands of criminals.

309. Because of the Data Breach, Plaintiff Kassem is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

310. Additionally, Plaintiff Kassem is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

311. Plaintiff Kassem stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently and periodically chooses unique usernames and passwords for his various online accounts.

312. Plaintiff Kassem has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants’ possession, is protected and safeguarded from future breaches.

Plaintiff Beth Berg’s Experience

313. Lakeview was the servicer for the residential mortgage on Plaintiff Berg’s home. As a condition to receiving loan services from Lakeview, Plaintiff Berg provided her PII which

was then entered into Lakeview's database and maintained by Lakeview on Bayview's network.

314. Plaintiff Berg greatly values her privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Berg took reasonable steps to maintain the confidentiality of her PII.

315. Plaintiff Berg received a letter dated March 21, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained 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.

316. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Berg faces, Defendant Lakeview offered her a one-year subscription to a credit monitoring service.

317. Following the Data Breach, an unauthorized individual opened a checking account in Plaintiff Berg's name with Bank of America. On or about March 4, 2022, Plaintiff Berg received a Bank of America credit card in the mail containing her name. Shortly after, Plaintiff Berg received a letter from Bank of America asking her to call the bank as a result of "suspicious activity." She later learned that someone obtained a cash advance in her name from Bank of America in the amount of \$3,500 (which included an additional \$200 in fees). This money was then deposited in the fraudulent checking account that had been opened in her name. Plaintiff Berg directed Bank of America to freeze the checking account and close the credit card. She then contacted credit reporting agencies and was told that if she did not make a payment on the fraudulently obtained credit card, her credit score would decrease by approximately 25 to 100 points. As a result, Plaintiff Berg was forced to make a payment of \$57 toward the credit card

balance to avoid a negative impact on her credit score. This payment was never refunded.

318. In February 2022, an unauthorized actor filed a 2021 federal tax return in her name and fraudulently obtained an approximately \$19,000 tax refund. The tax refund was deposited in an online bank account, which the unauthorized actor closed shortly thereafter. As a result, Plaintiff Berg was forced to file a corrected 2021 tax return, and she still has not received the tax refund owed to her. Plaintiff Berg had to schedule an in-office appointment to meet with an IRS agent regarding this fraud. During the appointment, she discovered that someone had also filed a claim for 2022 using her information.

319. On March 18, 2023, Plaintiff Berg was notified by email that BMO Bank declined an application for a checking account. On March 25, 2023, Plaintiff Berg received a letter from Barclays informing her of five checking accounts and five savings accounts fraudulently opened in her name on or around March 14, 2023.

320. Plaintiff Berg believes the fraud she suffered was a result of the Data Breach, including given the timing of the Data Breach, the types of data impacted, and her diligence in maintaining PII in a secure manner.

321. Plaintiff Berg was forced to spend significant time dealing with the fraudulent activity in her name, including approximately 80 phone calls with Bank of America, three trips to a local Bank of America branch (which required her to utilize her own vehicle and fuel), several communications with the IRS, and the filing of a police report. In total, Plaintiff Berg estimates that she spent over 100 hours dealing with the fraud committed against her.

322. Plaintiff Berg purchased layered protection ESET, which she renews for \$120 a year. After the Data Breach, in 2022, Plaintiff Berg added protection for her phone on her ESET plan.

323. Plaintiff Berg 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.

324. Plaintiff Berg also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant Lakeview in exchange for mortgage services.

325. Plaintiff Berg has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially with her Social Security number now in the hands of criminals.

326. Because of the Data Breach, Plaintiff Berg is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

327. Additionally, Plaintiff Berg is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Berg stores any documents containing her PII in a safe and secure location or destroys the documents.

328. Plaintiff Berg 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 Savannah Farley's Experience

329. Lakeview was the servicer for the residential mortgage on Plaintiff Farley's home. As a condition to receiving loan services from Lakeview, Plaintiff Farley provided her PII which was then entered into Lakeview's database and maintained by Lakeview on Bayview's network.

330. Plaintiff Farley greatly values her privacy and PII, especially in connection with

receiving loan and other financial services. Prior to the Data Breach, Plaintiff Farley took reasonable steps to maintain the confidentiality of her PII.

331. Plaintiff Farley received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained 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.

332. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Farley faces, Defendant Lakeview offered her a one-year subscription to a credit monitoring service. After receiving the letter, Plaintiff Farley signed up for this service. Plaintiff Farley also purchased credit monitoring through Experian, which required an initial payment of approximately \$30 and monthly charges thereafter of \$5.99.

333. In November 2021, Plaintiff Farley experienced fraud in the form of approximately 80 unauthorized charges on her credit card. Plaintiff Farley learned of this fraud after attempting to use her credit card and having her purchase declined as a result of the fraudulent activity, of which she previously had been unaware. Because her card was frozen as a result of the unauthorized charges, Plaintiff Farley was unable to purchase Easter gifts for her children. After learning of the fraudulent charges, she spent several hours communicating with her bank via phone and email over the course of several weeks. She was also required to take time off work to file a police report on or around April 27, 2022, concerning the fraud on her account. Plaintiff also placed a fraud alert on her Transunion account on April 27, 2022.

334. Plaintiff Farley believes the fraud was a result of the Data Breach given the timing, the type of data impacted, her diligence in maintaining her PII in a safe and secure manner, and

the fact that, to her knowledge, she has never before been a victim of identity theft or fraud.

335. Since learning of the Data Breach, Plaintiff Farley has spent (and will continue to spend) additional time reviewing her bank statements and credit cards. Plaintiff Farley expended this time at Lakeview's direction. In the notice letter Plaintiff Farley received, Lakeview directed Plaintiff Farley to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

336. Plaintiff Farley 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.

337. Plaintiff Farley also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant Lakeview in exchange for mortgage services.

338. Plaintiff Farley has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially with her Social Security number now in the hands of criminals.

339. Because of the Data Breach, Plaintiff Farley is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

340. Plaintiff Farley is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Farley stores any documents containing her PII in a safe and secure location or destroys the documents.

341. Plaintiff Farley 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 Thomas Lapenter's Experience

342. Plaintiff Lapenter took out a loan in or around December 2018 to purchase his home. The original loan servicer was Mr. Cooper. He then refinanced with Rocket Mortgage, from which Pingora purchased the mortgage. As a condition to providing Plaintiff Lapenter loan services, Pingora accessed his PII, which it then entered into its database and maintained on Bayview's network.

343. Plaintiff Lapenter greatly values his privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Lapenter took reasonable steps to maintain the confidentiality of his PII.

344. Plaintiff Lapenter received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network that contained his 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.

345. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Lapenter faces, Defendant Pingora offered him a one-year subscription to a credit monitoring service. Plaintiff Lapenter did not sign up for the subscription. Plaintiff Lapenter instead signed up and paid for a monthly subscription for identity protection services through LifeLock in or about April or May 2022. He also paid to have his credit frozen. Plaintiff purchased Discover credit monitoring services on April 19, 2022, and instituted a credit freeze.

346. Since October 2021, Plaintiff Lapenter has noticed suspicious bank activities and has had accounts opened under his name without authorization. Specifically, Plaintiff Lapenter learned that someone submitted a fraudulent loan application to his bank in his name when he

received a loan denial letter in the mail then contacted his bank. Plaintiff Lapenter received another letter from his bank on or around May 6, 2022, stating that the loan application had been investigated and was considered to be fraudulent. Plaintiff Lapenter reasonably believes that this fraudulent loan application was related to the Data Breach, including because it occurred just after the Data Breach. Also, the bank confirmed that the person used Plaintiff Lapenter's Social Security number on the application—information that was exposed in the Data Breach.

347. Plaintiff Lapenter has spent approximately 20 hours contacting credit bureaus, banks, freezing his credit, purchasing identity theft services that he trusts, and monitoring credit reports. Plaintiff Lapenter expended this time at Pingora's direction. In the notice letter Plaintiff Lapenter received, Pingora directed Plaintiff Lapenter to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

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

349. Plaintiff Lapenter also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant Pingora in exchange for mortgage services.

350. Plaintiff Lapenter has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially with his Social Security number now in the hands of criminals.

351. Because of the Data Breach, Plaintiff Lapenter is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

352. Additionally, Plaintiff Lapenter has spent \$15 per month on his identity theft

protection services, and he has also spent money to place credit freezes on his and his wife's credit reports. The credit freezes have made it more difficult for Plaintiff Lapenter to get loans for his business.

353. Plaintiff Lapenter is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

354. Plaintiff Lapenter stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently and periodically chooses unique usernames and passwords for his various online accounts.

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

Plaintiff Hardik Sevak's Experience

356. Plaintiff Sevak used Lakeview's services when Lakeview acquired his mortgage on his home in Floral Park, New York. As a condition to receiving loan services from Lakeview, Plaintiff Sevak's PII was provided to Lakeview, which was then entered into Lakeview's database and maintained by Lakeview on Bayview's network.

357. Plaintiff Sevak greatly values his privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Sevak took reasonable steps to maintain the confidentiality of his PII.

358. Plaintiff Sevak received a letter dated March 16, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained his name, address, loan number, and Social Security number.

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

Plaintiff Sevak faces, Defendant Lakeview offered him a one-year subscription to a credit monitoring service.

360. In December 2021, Plaintiff Sevak experienced identity fraud in the form of an unauthorized third party attempting to secure financing in his name from Synchrony Bank. As a result, he contacted the bank to stop the fraudulent activity. He believes the unauthorized financing is a result of the Data Breach given that it occurred after the Data Breach, and he had no other previous fraudulent activity. From December 2021 through June 2022, Plaintiff Sevak received four calls from Experian regarding unauthorized individuals who were attempting to open lines of credit in his name.

361. Since learning of the Data Breach Plaintiff Sevak has had to sign up for credit monitoring, identity theft and loss protection, including insurance against identity theft and identity restoration services. Plaintiff Sevak froze his credit shortly after the incident. He now uses services provided by Credit Karma, Experian, and Transunion to protect his identity.

362. Since learning of the Data Breach, Plaintiff Sevak has spent additional time reviewing his credit reports, bank statements and credit cards. Since the Data Breach, Plaintiff Sevak's information has been used by at least one unauthorized individual who attempted to open multiple fraudulent accounts and/or lines of credit in his name. As a result, he has spent approximately 250 hours resolving issues related to these fraudulent accounts, including but not limited to: reviewing his bank, credit and debit card statements; reviewing his emails for credit alerts; and reviewing his credit reports for any unauthorized charges. Plaintiff Sevak devoted this time at Lakeview's direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff Sevak to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

363. Plaintiff Sevak has experienced an increase in spam calls, text messages and emails since the Data Breach. The spam calls often included alarming personal details, which further contributed to Plaintiff Sevak's concern for his personal privacy and the safety of his identity. Moreover, following the Data Breach he received four phone calls from Experian regarding unauthorized individuals who were attempting to open lines of credit in his name.

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

365. Plaintiff Sevak also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant Lakeview in exchange for mortgage services.

366. Plaintiff Sevak has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially with his Social Security number now in the hands of criminals.

367. Because of the Data Breach, Plaintiff Sevak is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

368. Additionally, Plaintiff Sevak is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

369. Plaintiff Sevak stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently and periodically chooses unique usernames and passwords for his various online accounts.

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

Plaintiff Peter Wojciechowski's Experience

371. Plaintiff Wojciechowski took out a loan to purchase his home through Pulte Homes, a home builder. Lakeview purchased the mortgage two months later, in or around August 2021. As a condition to providing Plaintiff Wojciechowski loan services, Lakeview required access to his PII, which it then entered into its database and maintained on Bayview's network.

372. Plaintiff Wojciechowski greatly values his privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Wojciechowski took reasonable steps to maintain the confidentiality of his PII.

373. Plaintiff Wojciechowski received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained his 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.

374. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Wojciechowski faces, Defendant Lakeview offered him a one-year subscription to a credit monitoring service. Plaintiff Wojciechowski signed up for the one-year subscription on or around April 13, 2022. Plaintiff Wojciechowski placed a credit freeze with all three credit bureaus on or around May 19, 2022.

375. Plaintiff Wojciechowski experienced a fraud attempt on his United Services Automobile Association ("USAA") account where his name, date of birth, routing, and checking

account information were compromised.

376. Since October 2021, Plaintiff Wojciechowski has noticed suspicious bank activities. Specifically, he incurred a fraudulent Apple Store charge of \$708 on or around May 18, 2022. A woman in Florida used Plaintiff Wojciechowski's account and routing number to perform an electronic funds transfer and purchased an Apple iPhone. He discovered the unauthorized activity by checking his bank accounts every morning. He spent approximately 12 hours disputing the charge on the phone with USAA. On or around November 7, 2022, there was a fraudulent charge on Plaintiff's American Express card at a Sam's store in Arkansas for over \$520.

377. Plaintiff Wojciechowski spent approximately 12 hours with USAA related to the fraudulent ACH transaction, six hours freezing his credit, and approximately 70 hours actively monitoring his bank and credit card account information. Plaintiff Wojciechowski spent approximately four to five hours on the phone with American Express dealing with the fraudulent Sam's charge. He expended this time at Lakeview's direction. In the notice letter Plaintiff Wojciechowski received, Lakeview directed him to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

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

379. Plaintiff Wojciechowski also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant Lakeview in exchange for mortgage services.

380. Plaintiff Wojciechowski has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially

with his Social Security number now in the hands of criminals.

381. Because of the Data Breach, Plaintiff Wojciechowski is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

382. Additionally, Plaintiff Wojciechowski is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

383. Plaintiff Wojciechowski stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently and periodically chooses unique usernames and passwords for his various online accounts.

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

Plaintiff Kimberley Rowton's Experience

385. Plaintiff Rowton used Pingora's services when her home mortgage was transferred to Pingora. As a condition to receiving loan services from Pingora, Plaintiff Rowton's PII was provided to Pingora, which was then entered into Pingora's database and maintained by Pingora on Bayview's network.

386. Plaintiff Rowton greatly values her privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Rowton took reasonable steps to maintain the confidentiality of her PII.

387. Plaintiff Rowton received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network that contained 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.

388. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Rowton faces, Defendant Pingora offered her a one-year subscription to a credit monitoring service. Plaintiff Rowton signed up for the program on or around May 20, 2022, in an attempt to mitigate the harms she suffered as a result of the Data Breach. Plaintiff Rowton also placed a fraud alert on her credit through all three credit bureaus in early 2022. Plaintiff instituted a credit freeze with Transunion on April 19, 2022, with Experian on June 17, 2022, and with Equifax on January 28, 2022. Plaintiff Rowton signed up for an AOL Advantage Plan, for which she pays \$27.99 a month. On or around October 24, 2023, Plaintiff Rowton had to purchase another phone due to the large amount of spam she continued to receive.

389. An unauthorized person opened a cable account on or around November 18, 2022, in Plaintiff Rowton's name. She subsequently filed a police report.

390. Since the dates of the Data Breach, Plaintiff Rowton experienced identity fraud in the form of fraudulent transfers from her financial account. In January 2022, Plaintiff Rowton became aware that someone had used her PII to access one of her investment accounts and fraudulently transferred more than \$11,000 from it. Plaintiff Rowton contacted the investment institution to try to receive reimbursement and has filed a complaint with the FBI about the incident. To date, Plaintiff Rowton has not received reimbursement for the funds she lost due to the Data Breach. Plaintiff Rowton believes the fraudulent transfer of funds from her account using her PII is a result of the Data Breach given that it occurred relatively soon after the Data Breach and that she had never before experienced a fraudulent financial transfer.

391. On or around January 18, 2022, someone hacked into Plaintiff Rowton's cell phone account and paid with her saved credit card to switch access to another phone number and to

receive two-factor authentication codes. Plaintiff Rowton believes this incident was a result of the Data Breach given that it occurred relatively soon after the Data Breach and that she had never experienced a fraudulent financial transfer before.

392. In addition to the more than \$11,000 in funds that have been stolen from Plaintiff Rowton, she has also spent considerable time addressing the impacts of the Data Breach. Plaintiff Rowton estimates she has spent more than 40 hours responding to the Data Breach, including through attempting to receive reimbursement for her stolen funds; filing a report with the FBI about the fraudulent account transfer; signing up for credit monitoring; freezing her credit reports; reviewing her bank statements and other account statements; reviewing her credit monitoring reports; closely monitoring all activity involving her PII; and taking other necessary actions in response to the Data Breach.

393. Plaintiff Rowton expended this time at Pingora's direction. In the notice letter Plaintiff received, Pingora directed Plaintiff to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

394. Plaintiff Rowton had finally retired in August 2021 and is now concerned about her ability to provide for herself in the aftermath of having lost a considerable portion of her retirement savings.

395. Plaintiff Rowton 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.

396. Plaintiff Rowton also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant Pingora in exchange for mortgage services.

397. Plaintiff Rowton has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially with her Social Security number now in the hands of criminals.

398. Because of the Data Breach, Plaintiff Rowton is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

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

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

401. Plaintiff Rowton 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 Jessica Valente-Brodrick's Experience

402. Plaintiff Valente-Brodrick used Lakeview's services when she and her husband took out a mortgage on their home. As a condition to receiving loan services from Lakeview, Plaintiff Valente-Brodrick and her husband provided PII to Lakeview, which was then entered into Lakeview's database and maintained by Lakeview on Bayview's network.

403. Plaintiff Valente-Brodrick greatly values her privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Valente-Brodrick took reasonable steps to maintain the confidentiality of her PII.

404. Plaintiff Valente-Brodrick's husband received a letter dated March 16, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained

access to files on Lakeview's network that contained 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.

405. Recognizing the present, immediate, and substantially increased risk of harm she and her husband face, the Brodricks purchased identity theft monitoring prevention from Norton LifeLock which costs \$299.88 annually. Plaintiff Valente-Brodrick signed up for InfoArmor through Allstate on or around July 1, 2022.

406. In recent months, Plaintiff Valente-Brodrick has experienced identity fraud in the form of an unauthorized Wells Fargo account being opened in her name. She has also experienced several phishing attempts and suspicious activity, including receiving fake order and shipping alerts. She believes these events are a result of the Data Breach given that they occurred relatively soon after the Data Breach, and she had experienced no fraudulent activity or persistent phishing attempts prior to the Data Breach.

407. Since learning of the Data Breach, Plaintiff Valente-Brodrick has spent additional time reviewing her bank statements and credit cards. Moreover, Plaintiff expended this time at Lakeview's direction. In the notice letter her husband received, Lakeview directed Plaintiff Valente-Brodrick to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

408. Plaintiff Valente-Brodrick has experienced an increase in spam calls, text messages, and emails since the Data Breach.

409. Plaintiff Valente-Brodrick 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.

410. Plaintiff Valente-Brodrick also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant Lakeview in exchange for mortgage services.

411. Plaintiff Valente-Brodrick has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially with her Social Security number now in the hands of criminals.

412. Because of the Data Breach, Plaintiff Valente-Brodrick is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

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

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

415. Plaintiff Valente-Brodrick 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 Denise Scott's Experience

416. Plaintiff Scott used Lakeview's services when she took out a mortgage on her home. As a condition to receiving loan services from Lakeview, Plaintiff Scott provided Lakeview with her PII, which was then entered into Lakeview's database and maintained by Lakeview on Bayview's network.

417. Plaintiff Scott greatly values her privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Scott took reasonable steps

to maintain the confidentiality of her PII.

418. Plaintiff Scott received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained 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.

419. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Scott faces, Defendant Lakeview offered her a one-year subscription to a credit monitoring service.

420. In January 2022, Plaintiff Scott experienced identity fraud when someone fraudulently accessed her mortgage account and altered her payment settings. As a result, Plaintiff Scott received a letter from Lakeview that they were foreclosing on her home. Additionally, Plaintiff Scott incurred late fees totaling \$213.80.

421. In February 2022, Plaintiff Scott experienced additional identity fraud when someone attempted to charge \$790 on her American Express credit card. As a result, she spent time closing this card and replacing it. On April 15, 2022, Plaintiff Scott incurred an unauthorized charge of \$15 for an Amazon Prime account, even though she does not have such an account.

422. Since learning of the Data Breach, Plaintiff Scott has spent additional time reviewing her bank statements and credit cards. Since January 2022, she has spent approximately 40 hours dealing with the fraud attempts and attempting to mitigate the impacts of the Data Breach. Moreover, Plaintiff expended this time at Lakeview's direction. In the notice letter Plaintiff Scott received, Lakeview directed Plaintiff to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

423. On or around April 5, 2022, Plaintiff Scott instituted a credit freeze with Experian and Transunion.

424. Plaintiff Scott 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.

425. Plaintiff Scott also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant in exchange for mortgage services.

426. Plaintiff Scott has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially with her Social Security number now in the hands of criminals.

427. Because of the Data Breach, Plaintiff Scott is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

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

429. Plaintiff Scott stores any documents containing her PII in a safe and secure location or destroys the documents.

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

Plaintiff Nilsa Misencik's Experience

431. Plaintiff Misencik used Lakeview's services when she took out a mortgage on her home. As a condition to receiving loan services from Lakeview, Plaintiff Misencik provided

Lakeview with her PII, which was then entered into Lakeview's database and maintained by Lakeview on Bayview's network.

432. Plaintiff Misencik greatly values her privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Misencik took reasonable steps to maintain the confidentiality of her PII.

433. Plaintiff Misencik received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained 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.

434. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Misencik faces, Defendant Lakeview offered her a one-year subscription to a credit monitoring service.

435. On or around November 5, 2021, Plaintiff Misencik received a notification that a credit card she did not apply for had been denied. In November 2021, Plaintiff Misencik received a Montgomery Ward bill noting that someone in Miami was using her information. In February 2022, Plaintiff Misencik experienced identity fraud in the form of an unauthorized application and denial of a credit card from Bank of America. She believes the credit card application is a result of the Data Breach because it occurred relatively soon after the Data Breach.

436. Plaintiff Misencik also received a bill for an unauthorized purchase of a home appliance. Upon calling the biller, Plaintiff Misencik learned that the appliance seller had her date of birth, full name, Social Security number, address and phone number—information compromised in the Data Breach.

437. In or around January and February 2022, Plaintiff Misencik placed a fraud alert on her credit report. At or around that same time, Plaintiff Misencik instituted a credit freeze with Experian.

438. Since learning of the Data Breach, Plaintiff Misencik has spent additional time reviewing her bank statements and credit cards. Since February 2022, she has spent several hours reviewing her bank, credit and debit card statements; dealing with fraudulent purchases; and spending time on the phone dealing with the unauthorized credit card application and other unauthorized charges. Plaintiff expended this time at Lakeview's direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

439. Plaintiff Misencik 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.

440. Plaintiff Misencik also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant Lakeview in exchange for mortgage services.

441. Plaintiff Misencik has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially with her Social Security number now in the hands of criminals.

442. Because of the Data Breach, Plaintiff Misencik is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

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

444. Plaintiff Misencik 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 David Kraus's Experience

445. Plaintiff Kraus used Pingora's services when he took out a mortgage on his home. As a condition to receiving loan services from Pingora, Plaintiff Kraus provided Pingora with his PII, which was then entered into Pingora's database and maintained by Pingora on Bayview's network.

446. Plaintiff Kraus greatly values his privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Kraus took reasonable steps to maintain the confidentiality of his PII.

447. Plaintiff Kraus received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network that contained his 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.

448. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Kraus faces, Defendant Pingora offered him a one-year subscription to a credit monitoring service.

449. In April 2022, Plaintiff Kraus experienced identity fraud in the form of unauthorized charges on his credit card in the amount of \$250 and \$2,563. As a result, he had to obtain a new card. On or around April 13, 2022, Plaintiff Kraus received a call from his bank notifying him that his credit card was used without his authorization. He believes the unauthorized

charges on his debit card are a result of the Data Breach because they occurred relatively soon after the Data Breach, and he had no other previous fraudulent charges on his card.

450. On or around April 13, 2022, Plaintiff Kraus's computer was hacked and its operation held hostage by ransomware.

451. Plaintiff Kraus placed a fraud alert on his credit through Transunion on or around April 19, 2022.

452. Since learning of the Data Breach, Plaintiff Kraus has spent additional time reviewing his bank statements and credit cards. Since February 2022, he has spent approximately 40 hours reviewing his bank, credit, and debit card statements; procuring a new credit card; speaking with government officials; and speaking with bank employees. Plaintiff Kraus expended this time at Pingora's direction. In the notice letter Plaintiff received, Pingora directed Plaintiff to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

453. Plaintiff Kraus has experienced an increase in spam calls, text messages and emails since the Data Breach.

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

455. Plaintiff Kraus also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant Pingora in exchange for mortgage services.

456. Plaintiff Kraus has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially

with his Social Security number now in the hands of criminals.

457. Because of the Data Breach, Plaintiff Kraus is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

458. Additionally, Plaintiff Kraus is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

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

Plaintiff John McMahon's Experience

460. Plaintiff McMahon used Lakeview's services when he took out a mortgage on his home. As a condition to receiving loan services from Lakeview, Plaintiff McMahon provided Lakeview with his PII, which was then entered into Lakeview's database and maintained by Lakeview on Bayview's network.

461. Plaintiff McMahon greatly values his privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff McMahon took reasonable steps to maintain the confidentiality of his PII.

462. Plaintiff McMahon received a letter dated March 16, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained his 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.

463. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff McMahon faces, Defendant Lakeview offered him a one-year subscription to a credit monitoring service. After receiving the letter, Plaintiff McMahon signed up for this service.

464. On January 25, 2022, Plaintiff McMahon received a notification from the credit monitoring service that he maintained through Discover informing him that his Social Security number was “compromised.” The alert further stated: “We have located your Social Security number on a Dark Web site.” Plaintiff believes that this was a result of the Data Breach given the timing of the notification, his diligence in storing and maintaining his PII in a secure manner, and the fact that, to his knowledge, he has not been the subject of any other data breaches involving his Social Security number.

465. As a result of the Data Breach and notification that his PII is on the dark web, Plaintiff McMahon was forced to cancel all of his credit cards and have them reissued, a process that took significant time.

466. Since learning of the Data Breach, Plaintiff McMahon has suffered a further loss of time (and continues to spend a considerable amount of time) on issues related to this Data Breach, such as monitoring accounts and credit scores. He also spent considerable time implementing an alert with one of the major credit bureaus, and intends to spend time taking additional steps to protect his PII. Plaintiff expended this time at Lakeview’s direction. In the notice letter Plaintiff McMahon received, Lakeview directed him to spend time mitigating his losses by “reviewing your account statements and free credit reports for unauthorized activity.”

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

468. Plaintiff McMahon also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant Lakeview in exchange for mortgage services.

469. Plaintiff McMahon has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially with his Social Security number now in the hands of criminals.

470. Because of the Data Breach, Plaintiff McMahon is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

471. Plaintiff McMahon is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

472. Plaintiff McMahon stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently and periodically chooses unique usernames and passwords for his various online accounts.

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

Plaintiff Shannon Thomas's Experience

474. Plaintiff Thomas took out a mortgage loan for property in Ohio. At all times relevant to this Complaint, Defendant Lakeview was the servicer of Plaintiff Thomas's mortgage loan. As a condition to providing Plaintiff Thomas loan services, Lakeview accessed Plaintiff Thomas's PII, which it then entered into its database and maintained on Bayview's network.

475. Plaintiff Thomas greatly values her privacy and PII, especially in connection with receiving loan and financial services. Plaintiff Thomas takes reasonable steps to maintain the

confidentiality of her PII.

476. Plaintiff Thomas received a letter on or around March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained 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.

477. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Thomas faces, Defendant Lakeview offered her a one-year subscription to a credit monitoring service.

478. Plaintiff Thomas signed up for Norton LifeLock on or around March 30, 2022, for which she originally paid \$15.99 per month. Her payments have since increased to \$24.99 per month.

479. Since October 2021, as a direct result of the Data Breach, Plaintiff Thomas has already had to spend time and energy protecting and monitoring her identity and credit. Plaintiff Thomas spent time reviewing bank accounts and statements, changing passwords related to her business and personal accounts, reviewing her credit reports from all three credit bureaus, and she will have to spend additional time and energy in the future continuing to monitor and protect her identity and credit. Plaintiff Thomas expended this time at Lakeview's direction. In the notice letter Plaintiff Thomas received, Defendant Lakeview directed her to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

480. Additionally, Plaintiff Thomas has spent money out of pocket to address the Data Breach, including by purchasing LifeLock Advantage.

481. Plaintiff Thomas has experienced an increase in spam calls, text messages, and

emails since the Data Breach.

482. Plaintiff Thomas 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.

483. Plaintiff Thomas also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant Lakeview in exchange for mortgage services.

484. Plaintiff Thomas has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially with her Social Security number now in the hands of criminals.

485. Because of the Data Breach, Plaintiff Thomas is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

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

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

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

Plaintiff Mathew Myers's Experience

489. Plaintiff Myers used Lakeview's services when Lakeview acquired his mortgage on his home in August 2019. As a condition to receiving loan services from Lakeview, Plaintiff

Myers's PII was provided to Lakeview, which was then entered into Lakeview's database and maintained by Lakeview on Bayview's network.

490. Plaintiff Myers greatly values his privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Myers took reasonable steps to maintain the confidentiality of his PII.

491. Plaintiff Myers received a letter dated March 18, 2022 from Defendant Lakeview concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Lakeview's network that contained his 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.

492. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Myers faces, Defendant Lakeview offered him a one-year subscription to a credit monitoring service. Plaintiff Myers has not signed up for the program, as he does not trust that Lakeview's chosen vendor can protect his information. He instead signed up for credit monitoring and identity theft protection services through LifeLock, Credit Karma, Transunion, and Norton in order to protect his information. Plaintiff Myers signed up for LifeLock in April 2022, for which he pays \$17.31 a month. He signed up for Nomorobo on or around May 24, 2022, for which he pays \$19.99 a year. Plaintiff froze his credit on or around May 18, 2022. Plaintiff then unfroze his credit on or around July 26, 2022, to shop for mortgages, and refroze his credit on February 14, 2023.

493. Further, since learning of the Data Breach, Plaintiff Myers has spent additional time reviewing his credit reports, bank statements and credit cards. Since April 2022, he has spent approximately one to two hours every day reviewing his bank, credit and debit card statements;

reviewing his emails for credit alerts; and reviewing his credit reports for any unauthorized charges. Moreover, Plaintiff expended this time at Lakeview's direction. In the notice letter Plaintiff received, Lakeview directed Plaintiff to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

494. Plaintiff Myers has experienced an increase in spam calls, text messages, and emails since the Data Breach.

495. As a result of the Data Breach, Plaintiff Myers had to sign up and pay for the service "Nomorobo" to address the influx of spam calls, at a cost of \$19.99 per year.

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

497. Plaintiff Myers also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant Lakeview in exchange for mortgage services.

498. Plaintiff Myers has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially with his Social Security number now in the hands of criminals.

499. Because of the Data Breach, Plaintiff Myers is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

500. Additionally, Plaintiff Myers is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

501. Plaintiff Myers stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently and periodically chooses unique

usernames and passwords for his various online accounts.

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

Plaintiff Jay Saporta's Experience

503. Plaintiff Saporta originally secured a mortgage for his home from Mutual of Omaha, and the mortgage was originally serviced by PHH Mortgage. Plaintiff only became aware that Pingora had acquired his PII after he received the April 6, 2022 letter from Pingora alerting him that his PII had been compromised in the Data Breach. As a condition to providing Plaintiff Saporta loan services, Pingora required access to his PII, which it received and entered into its database to maintain on Bayview's network.

504. Plaintiff Saporta greatly values his privacy and the confidentiality of his PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Saporta took reasonable steps to maintain the confidentiality of his PII.

505. Plaintiff Saporta received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network that contained his 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.

506. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Saporta faces, Defendant Pingora offered him a one-year subscription to a credit monitoring service.

507. In or around May 2022, Plaintiff Saporta learned from TurboTax that his

information had appeared on the dark web.

508. Since learning of the Data Breach, Plaintiff Saporta took considerable efforts to mitigate its impact—at Defendant Pingora’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 three credit report agencies due to the Data Breach, which costs him approximately \$15 per month; and reviewing the credit monitoring service offered by Pingora. Plaintiff Saporta activated Credit Lock on or around April 10, 2022. He also froze his credit on or around April 10, 2022.

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

510. Plaintiff Saporta also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant Pingora in exchange for mortgage services.

511. Plaintiff Saporta has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially with his Social Security number now in the hands of criminals.

512. Because of the Data Breach, Plaintiff Saporta is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

513. Additionally, Plaintiff Saporta is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

514. Plaintiff Saporta stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently and periodically chooses unique

usernames and passwords for his various online accounts.

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

516. Pursuant to § 1798.150(b) of the CCPA, Plaintiff Jay Saporta gave written notice to Defendants Bayview and Pingora of their specific violations of § 1798.150(a) by certified mail dated April 14, 2022. Pingora responded on April 29, 2022 but failed to cure. Bayview has not responded.

Plaintiff Albert Brumitt's Experience

517. Defendant Community Loan is the servicer of Plaintiff Brumitt's mortgage loan. As a condition to receiving loan services from his Community Loan, Plaintiff Brumitt provided Community Loan with his PII, which was then entered into Community Loan's database and maintained by Community Loan on Bayview's network.

518. Plaintiff Brumitt greatly values his privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Brumitt took reasonable steps to maintain the confidentiality of his PII.

519. Plaintiff Brumitt received a letter dated August 16, 2022, from Defendant Community Loan concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Community Loan's network. The compromised files contained his name and Social Security number, and, potentially, information he provided in connection with a loan application, loan modification, or other items regarding loan servicing.

520. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Brumitt faces, Defendant Community Loan offered him a one-year subscription to a credit

monitoring service.

521. Since learning of the Data Breach, Plaintiff Brumitt has spent additional time reviewing his bank statements and credit cards. Nearly every single day since learning of the Breach, Plaintiff calls his bank and reviews his financial records and all charges with the clerk. This process takes roughly an hour every day. Plaintiff Brumitt expended this time at Community Loan's direction. In the notice letter he received, Community Loan directed Plaintiff to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

522. Plaintiff Brumitt has also experienced an increase in spam calls, text messages, and emails since the Data Breach.

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

524. Plaintiff Brumitt also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant Community Loan in exchange for mortgage services.

525. Plaintiff Brumitt has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially with his Social Security number now in the hands of criminals.

526. Because of the Data Breach, Plaintiff Brumitt is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

527. Additionally, Plaintiff Brumitt is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

528. Plaintiff Brumitt stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently and periodically chooses unique usernames and passwords for his various online accounts.

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

Plaintiff David Cunningham's Experience

530. Defendant Community Loan is the servicer of Plaintiff Cunningham's mortgage loan. As a condition to receiving loan services from his Community Loan, Plaintiff Cunningham provided Community Loan with his PII, which was then entered into Community Loan's database and maintained by Community Loan on Bayview's network.

531. Plaintiff Cunningham greatly values his privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Cunningham took reasonable steps to maintain the confidentiality of his PII.

532. Plaintiff Cunningham received a letter dated October 17, 2022 from Defendant Community Loan concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Community Loan's network. The compromised files contained his name and Social Security number, and, potentially, information he provided in connection with a loan application, loan modification, or other items regarding loan servicing.

533. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Cunningham faces, Defendant Community Loan offered him a one-year subscription to a credit monitoring service.

534. After the Data Breach, Plaintiff Cunningham experienced identity fraud. In or

around January 2023, an unauthorized person attempted to open a Bank of America account in Plaintiff Cunningham's name. Plaintiff Cunningham believes this to be a result of the Data Breach due to the proximity in time.

535. Since learning of the Data Breach, Plaintiff Cunningham has spent additional time reviewing his bank statements and credit cards. Plaintiff Cunningham expended this time at Community Loan's direction. In the notice letter Plaintiff Cunningham received, Community Loan directed Plaintiff to spend time mitigating his losses by "reviewing your account statements and free credit reports for unauthorized activity."

536. Plaintiff Cunningham has experienced an increase in spam calls, text messages, and emails since the Data Breach.

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

538. Plaintiff Cunningham also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant Community Loan in exchange for mortgage services.

539. Plaintiff Cunningham has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially with his Social Security number now in the hands of criminals.

540. Because of the Data Breach, Plaintiff Cunningham is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

541. Additionally, Plaintiff Cunningham is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

542. Plaintiff Cunningham stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently and periodically chooses unique usernames and passwords for his various online accounts.

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

Plaintiff Linda Kim's Experience

544. As a condition to receiving loan services from her mortgage originator and servicers, whom Plaintiff Linda Kim believes provided her PII to Community Loan, she provided her PII to those mortgage originators and servicers, which they provided to Community Loan. Her PII was then entered into Community Loan's database and maintained by Community Loan on Bayview's network.

545. Plaintiff Kim greatly values her privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Kim took reasonable steps to maintain the confidentiality of her PII.

546. Plaintiff Kim received a letter dated October 17, 2022 from Defendant Community Loan concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Community Loan's file servers. The compromised files contained her name and Social Security number, and may have also included information Plaintiff Kim provided in connection with a loan application, loan modification, or other items regarding loan servicing.

547. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Kim faces, Defendant Community Loan offered her a one-year subscription to a credit

monitoring service. Plaintiff Kim has signed up for the program but does not believe this is sufficient to protect her identity from the ongoing risks of fraud and theft she faces.

548. Since learning of the Data Breach, Plaintiff Kim has spent additional time reviewing her bank statements, credit cards, and reviewing her emails for fraud alerts. Since October 2022, she has spent several hours in total reviewing her bank, credit and debit card statements; and reviewing her emails for fraud alerts or otherwise suspicious account activity. Moreover, Plaintiff expended this time at Community Loan's direction. In the notice letter Plaintiff received, Community Loan directed Plaintiff to spend time mitigating her losses by "reviewing [her] account statements and free credit reports for unauthorized activity."

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

550. Plaintiff Kim 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.

551. Plaintiff Kim also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant Community Loan in exchange for mortgage services.

552. Plaintiff Kim has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially with her Social Security number now in the hands of criminals.

553. Because of the Data Breach, Plaintiff Kim is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

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

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

556. Plaintiff Kim 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.

557. On October 31, 2022 Plaintiff Kim transmitted a 30-day Notice of Claim pursuant to Cal. Civ. Code § 1798.150 to Defendants Bayview and Community Loan alleging they violated the CCPA and demanding they cure such violation within 30 calendar days of the date of her Notice of Claim. Although Bayview and Community Loan responded to Plaintiff Kim's Notice of Claim, they did not cure their CCPA violations.

Plaintiff Maureen Keach's Experience

558. Plaintiff Maureen Keach never used Pingora's services when she took out a mortgage on her home. To her knowledge, Pingora has never serviced her mortgage and she has never willingly provided any of her PII to Pingora.

559. As a condition to receiving loan services from her mortgage originator and servicers, whom she believes provided her PII to Pingora, Plaintiff Keach provided her PII to those mortgage originators and servicers, which they provided to Pingora. The PII was then entered into Pingora's database and maintained by Pingora on Bayview's network.

560. Plaintiff Keach greatly values her privacy and PII, especially in connection with receiving loan and financial services. Prior to the Data Breach, Plaintiff Keach took reasonable

steps to maintain the confidentiality of her PII.

561. Plaintiff Keach received a letter dated April 6, 2022 from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network that contained 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.

562. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Keach faces, Defendant Pingora offered her a one-year subscription to a credit monitoring service. Plaintiff Keach has signed up for the program but does not believe this is sufficient to protect her identity from the ongoing risks of theft she faces.

563. In December 2021, Plaintiff Keach experienced identity fraud in the form of an unauthorized \$413 charge for a "security plan" through "Geek Squad"; she also received an unauthorized \$451 bill for MacAfee service at approximately the same time; and in April 2022 incurred an unauthorized charge of \$284.99 from Norton LifeLock. She believes these unauthorized charges are a result of the Data Breach given that they occurred relatively soon after the Data Breach, and she experienced no previous fraudulent charges.

564. Since learning of the Data Breach, Plaintiff Keach has spent additional time reviewing her bank statements, credit cards, and reviewing her emails for fraud alerts. Since April 2022, she has spent approximately one hour every day reviewing her bank, credit and debit card statements, and reviewing her emails for fraud alerts or otherwise suspicious account activity. Moreover, Plaintiff Keach expended this time at Pingora's direction. In the notice letter Plaintiff Keach received, Pingora directed Plaintiff to spend time mitigating her losses by "reviewing your account statements and free credit reports for unauthorized activity."

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

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

567. Plaintiff Keach 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.

568. Plaintiff Keach also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant Pingora in exchange for mortgage services.

569. Plaintiff Keach has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially with her Social Security number now in the hands of criminals.

570. Because of the Data Breach, Plaintiff Keach is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

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

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

573. Plaintiff Keach 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.

574. On April 14, 2022, Plaintiff Keach transmitted a 30-day Notice of Claim pursuant to Cal. Civ. Code § 1798.150 to Defendants Bayview and Pingora alleging they violated the CCPA and demanding they cure such violation within 30 calendar days of the date of her Notice of Claim. Pingora responded to the Notice of Claim but did not cure its CCPA violations.

575. Bayview never responded to Plaintiff Keach's Notice of Claim.

Plaintiff Pedro Rubio's Experience

576. Plaintiff Pedro Rubio took out a loan to purchase his home. The original servicer of Plaintiff Rubio's mortgage was Lakeview. As a condition to providing Plaintiff Rubio mortgage services, Lakeview required access to his personal information and PII, including but not limited to his name, marital status, date of birth, Social Security number, employment information, and other common items asked when applying for credit. This PII was entered into and maintained in Lakeview's database on Bayview's network.

577. Plaintiff Rubio greatly values his privacy and PII, especially in connection with receiving financial services, including loan or mortgage services. Prior to the Data Breach, Plaintiff Rubio took reasonable steps to maintain the confidentiality of his PII.

578. Plaintiff Rubio received a letter dated March 17, 2022 from Defendant Lakeview concerning the Data Breach. The letter from Lakeview stated that unauthorized actors gained access to files on Lakeview's network in early December 2021. The compromised files contained Plaintiff Rubio's 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.

579. Recognizing the present, immediate, and substantially increased risk of harm, including fraud and identity theft, which Plaintiff Rubio now faces as a result of the Data Breach,

Defendant Lakeview's letter offered a one-year membership to a third-party identity monitoring service. Plaintiff Rubio elected not to sign up for the identity monitoring service offered in Lakeview's letter.

580. Since learning of the Data Breach, Plaintiff Rubio has spent additional time reviewing his bank statements, credit cards, and financial accounts. Plaintiff Rubio has spent time reviewing his accounts and credit information, and spent time to freeze his credit to mitigate damages caused by the Data Breach. He expended this time, which would otherwise be spent on other activities, at Lakeview's direction, as the notice letter he received from Lakeview directed him to spend time mitigating his damages by "reviewing your account statements and free credit reports for unauthorized activity."

581. Plaintiff Rubio also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant Pingora in exchange for mortgage services.

582. Plaintiff Rubio has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially with her Social Security number now in the hands of criminals.

583. Plaintiff Rubio believed his PII 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 is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

584. Plaintiff Rubio plans to spend additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts and credit information for any unauthorized activity.

585. Plaintiff Rubio also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant Lakeview in order to obtain services from Defendant Lakeview, which was compromised in and as a result of the Data Breach.

586. Plaintiff Rubio has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially with his Social Security number now in the hands of criminals.

587. Because of the Data Breach, Plaintiff Rubio is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

588. Plaintiff Rubio is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

589. Plaintiff Rubio stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he chooses unique usernames and passwords for his various online accounts.

590. Plaintiff Rubio has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future data breaches and unauthorized access, disclosure, and/or exfiltration to unauthorized third parties.

591. Pursuant to § 1798.150(b) of the CCPA, Plaintiff Rubio gave written notice to Defendant Lakeview of its specific violations of § 1798.150(a) by certified mail dated April 13, 2022. Lakeview responded on April 29, 2022 but failed to cure.

Plaintiff Norma Grossman's Experience

592. Plaintiff Grossman took out a loan to purchase her home. The original servicer was Alterra Home Loans, a subsidiary of Panorama Mortgage Group, LLC. At some point Pingora acquired Plaintiff Grossman's home mortgage. As a condition to receiving loan services from Pingora, Plaintiff Grossman's PII was provided to Pingora, which was then entered into Pingora's database and maintained by Pingora on Bayview's network.

593. Plaintiff Grossman greatly values her privacy and PII, especially in connection with receiving loan and other financial services. Prior to the Data Breach, Plaintiff Grossman took reasonable steps to maintain the confidentiality of her PII.

594. Plaintiff Grossman received a letter dated April 6, 2022, from Defendant Pingora concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Pingora's network that contained 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.

595. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Grossman faces, Defendant Pingora offered her a one-year subscription to a credit monitoring service. Plaintiff Grossman signed up for the program in an attempt to mitigate the harms he suffered as a result of the Data Breach.

596. Since the Data Breach, Plaintiff Grossman estimates that she has spent at least 10 hours responding to the Data Breach, including reviewing bank statements and other financial documents, as well as driving to the bank to change her financial account information that was exposed in the Data Breach. This time was spent at Pingora's direction in the Notice Letter, in

which Pingora directed Plaintiff “to be vigilant for incidents of fraud or identity theft by reviewing your account statements”

597. Plaintiff Grossman 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.

598. Plaintiff Grossman also suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant Pingora in order to obtain services from Defendant Pingora, which was compromised in and as a result of the Data Breach.

599. Plaintiff Grossman has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially with her Social Security number now in the hands of criminals.

600. Because of the Data Breach, Plaintiff Grossman is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

601. Plaintiff Grossman is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

602. Plaintiff Grossman stores any documents containing her PII in a safe and secure location and destroy the documents when she no longer needs them. Moreover, she diligently and periodically chooses unique usernames and passwords for her various online accounts.

603. Plaintiff Grossman 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.

604. Pursuant to § 1798.150(b) of the CCPA, Plaintiff Norma Grossman gave written notice to Defendant Pingora of its specific violations of § 1798.150(a) by certified mail dated June 6, 2022. Pingora has not responded.

Plaintiffs' Injuries and Damages

605. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members are presently experiencing and will continue experiencing actual harm from fraud and identity theft.

606. Plaintiffs and Class Members are presently experiencing substantial risk of out-of-pocket fraud losses, such as loans and accounts opened in their names, fraudulent charges, tax return fraud, utility bills opened in their names, and similar identity theft.

607. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

608. Plaintiffs and Class Members are also incurring, and may continue incurring for the remainder of their lifetimes, out-of-pocket costs for protective measures such as identity theft protection and credit monitoring fees (for any credit monitoring obtained in addition to or in lieu of the inadequate monitoring offered by Defendants), credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

609. Plaintiffs and Class Members also suffered damage to or depreciation of their PII when it was acquired by the cyber thieves in the Data Breach. Numerous courts have recognized such damages in cases such as this one.

610. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and other accounts and records for misuse. Defendants'

own notice of data breach instructs Plaintiffs and Class Members regarding the time that they will need to spend monitoring their own accounts and statements.

611. Plaintiffs and Class Members have suffered actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- a. Finding fraudulent loans, insurance claims, tax returns, and/or government benefit claims;
- b. Purchasing credit monitoring and identity theft prevention;
- c. Placing “freezes” and “alerts” with credit reporting agencies;
- d. Spending time on the phone with or at a financial institution or government agency to dispute fraudulent charges and/or claims;
- e. Contacting financial institutions and closing or modifying financial accounts; and
- f. Closely reviewing and monitoring Social Security, medical insurance accounts, bank accounts, payment card statements, and credit reports for unauthorized activity for years to come.

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

613. As a direct and proximate result of Defendants' actions and inaction, Plaintiffs and Class Members have suffered a loss of privacy and face a substantial and present risk of harm.

VI. CLASS ALLEGATIONS

614. 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 bring this Action on behalf of themselves and the following Class and constituent Subclasses, subject to amendment as appropriate:

All individuals in the United States whose PII was accessed or exfiltrated during the Data Breach (the "Class");

All individuals residing in California whose PII was accessed or exfiltrated during the Data Breach (the "California Subclass");

All individuals residing in Florida whose PII was accessed or exfiltrated during the Data Breach (the "Florida Subclass");

All individuals residing in Illinois whose PII was accessed or exfiltrated during the Data Breach (the "Illinois Subclass");

All individuals residing in New York whose PII was accessed or exfiltrated during the Data Breach (the "New York Subclass");

All individuals residing in Washington whose PII was accessed or exfiltrated during the Data Breach (the "Washington Subclass").

615. Excluded from the Class and the Subclasses are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, members, 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.

616. Plaintiffs reserve the right to modify or amend the definitions of the Class and

Subclasses before the Court determines whether class certification is appropriate.

617. Numerosity. Consistent with Fed. R. Civ. P. 23(a)(1), the Class Members are so numerous that their joinder is impracticable. Defendants' public statements indicate that the number of Class Members exceeds two and a half million. The number and identities of Class Members can be readily ascertained through Defendants' records.

618. 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 questions include, without limitation:

- 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 to an unauthorized third party;
- 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 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;
- h. Whether Defendants have adequately addressed and fixed the vulnerabilities which

permitted the Data Breach to occur;

- i. Whether Defendants Lakeview, Community Loan, and Pingora breached contracts with other entities, the terms and conditions of which provide for the safeguarding of Plaintiffs' and Class Members' PII for their benefit;
- j. Whether Defendants engaged in unfair, unlawful, or deceptive practices, including by failing to safeguard the PII of Plaintiffs and Class Members;
- k. Whether Bayview violated state statutes as alleged herein;
- l. Whether Lakeview violated state statutes as alleged herein;
- m. Whether Community Loan violated state statutes as alleged herein;
- n. Whether Pingora violated state statutes as alleged herein;
- o. Whether Plaintiffs and Class Members are entitled to damages or restitution as a result of Defendants' wrongful conduct; and
- p. 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.

619. 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 in the Data Breach due to Defendants' unlawful conduct, and their claims arise under the same legal doctrines.

620. Conduct Generally Applicable to the Class. As provided under Fed. R. Civ. P. 23(b)(2), Defendants have acted or failed to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible, compliant 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.

621. 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 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.

622. 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.

623. 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 will materially advance the resolution of this matter and the parties' interests therein.

624. 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.

625. Certification of subclasses under Fed. R. Civ. P. 23(c)(5) also is warranted. Certification of the Subclasses defined in this Complaint will ensure that each of the different counts proceeds against the appropriate Defendant(s) and that claims arising under state statutes are brought on behalf of Class Members residing in those states.

COUNT I
NEGLIGENCE
On Behalf of All Plaintiffs and the Class or, Alternatively, the Subclasses
Against All Defendants

626. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 625.

All Defendants—Foreseeability

627. Prior to the Data Breach, each Defendant knew or should have known that threat attackers were targeting banks and other financial services entities such as Defendants in an effort to obtain personally identifiable information and misuse it to commit fraud and identity theft, particularly when stored in an internet-accessible environment, in at least the following respects:

- a. Bayview, Lakeview, Pingora, and Community Loan were aware of previous data breaches that had targeted banks and mortgage providers, including breaches that affected information of their own customers;
- b. Hackers are known to routinely attempt to steal such information and use it for nefarious purposes; and

- c. Publicly available industry warnings regarding threat attackers' efforts to obtain such information for ransom or misuse were widely and readily available to Defendants.

Bayview—Duty, Breach, and Causation

628. Prior to the Data Breach, Bayview knowingly and intentionally acquired the PII of Plaintiffs and Class Members, including their Social Security numbers, from Lakeview, Community Loan, Pingora, and others.

629. In knowingly and intentionally acquiring the PII of Plaintiffs and Class Members, Bayview assumed a duty to use reasonable care, including implementing reasonable security practices and procedures, to safeguard the PII of Plaintiffs and Class Members against unauthorized access, acquisition, and misuse.

630. Bayview failed to use reasonable care by storing the PII of Plaintiffs and Class Members in an internet-accessible environment under the following circumstances:

- a. The PII of Plaintiffs and Class Members was not encrypted.
- b. The PII of Plaintiffs and Class Members that Defendants had no reasonable need to store in an internet-accessible environment, including the PII of Plaintiffs and Class Members with whom Defendants had not had a relationship for years, was not removed from Defendants' network.
- c. The movement of the PII of Plaintiffs and Class Members from Bayview's network to the internet was not monitored and detected in real time.
- d. Bayview failed to include CobaltStrike on the emergency threat feed or test its "use cases," allowing the threat attacker to remain on Bayview's network undetected.

- e. Sentinel One—the all-important threat detection and response tool—was not feeding into Bayview’s SIEM System.

631. Under like circumstances, a reasonably careful person would have done the following:

- a. Encrypted the PII.
- b. Removed from Defendant’s network the PII that Defendant had no reasonable need to store in an internet-accessible environment, including the PII of individuals with whom Defendant had not had a relationship for years.
- c. Monitored and detected in real time the movement of the PII from the network to the internet.
- d. Included CobaltStrike on the emergency threat feed or tested its “use cases,” thereby preventing the threat attacker from remaining on the network undetected.
- e. Ensured Sentinel One was feeding into the SIEM system.

632. Bayview’s conduct also constituted negligence per se. As stated herein, Bayview is a financial institution subject to the requirements of the GLBA, 15 U.S.C. § 6801, *et seq.*, and the FTC Act, 15 U.S.C. § 41, *et seq.* The GLBA required Bayview to take several preventive security measures to protect Plaintiffs’ and Class Members’ data, including:

- a. maintaining an adequate data security system to reduce the risk of data breaches and cyber attacks;
- b. adequately protecting Plaintiffs’ and Class Members’ PII;
- c. implementing policies and procedures to prevent, detect, contain, and correct security violations;

- d. implementing procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports;
- e. protecting against any reasonably anticipated threats or hazards to the security or integrity of PII; and
- f. effectively training all members of their workforce on the policies and procedures with respect to PII as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of PII.

633. By failing to take the above security measures, Bayview breached duties imposed under federal law, rules, and regulations.

634. Bayview's negligence directly and in natural and continuous sequence produced or contributed substantially to producing Plaintiffs' and Class Members' damage because of the following:

- a. Bayview's failure to encrypt the PII of Plaintiffs and Class Members allowed the threat attacker to acquire their PII.
- b. Bayview's failure to remove from Defendants' network the PII of Plaintiffs and Class Members that Defendants had no reasonable need to store in an internet-accessible environment, including the PII of Plaintiffs and Class Members with whom Defendants had not had a relationship for years, allowed the threat attacker to acquire their PII.
- c. Bayview's failure to monitor in real time the movement of the PII of Plaintiffs and Class Members from Bayview's network to the internet allowed the threat attacker to exfiltrate the PII without detection and therefore without any attempt to halt the exfiltration before its completion.

- d. Bayview's failure to include CobaltStrike on the emergency threat feed or test its "use cases," allowed the threat attacker to remain on the network undetected.
- e. Bayview's failure to ensure Sentinel One was feeding into Bayview's SIEM system impeded the detection of CobaltStrike activity.

635. But for Bayview's negligence, the damage to Plaintiffs and Class Members would not have occurred because of the following:

- a. If Bayview had encrypted the PII of Plaintiff and Class Members, the threat attacker would not have acquired their PII.
- b. If Bayview had removed from Defendants' network the PII of Plaintiffs and Class Members that Defendants had no reasonable need to store in an internet-accessible environment, the threat attacker would not have acquired their PII.
- c. If Bayview had monitored in real time the movement of the PII of Plaintiffs and Class Members from Defendant's network to the internet, the exfiltration of the PII could have been halted before its completion.
- d. If Bayview had included CobaltStrike on the emergency threat feed or tested its "use cases," the threat attacker would have been prevented from remaining on the network undetected.
- e. If Bayview had ensured Sentinel One was feeding into Bayview's SIEM, the CobaltStrike activity would have been detected.

636. Bayview's negligence was a legal cause of damage to Plaintiffs and Class Members, even if it operated in combination with the acts of the threat attacker, because the acts

of and the harmed caused by the threat attacker were reasonably foreseeable, and Bayview's negligence contributed substantially to producing such damage to Plaintiffs and Class Members.

Lakeview—Duty, Breach, and Causation

637. Prior to the Data Breach, Lakeview knowingly and intentionally acquired the PII of Plaintiffs and Class Members, including their Social Security numbers, either directly or indirectly from Plaintiffs and Class Members.

638. In knowingly and intentionally entrusting the PII of Plaintiffs and Class Members to Bayview and relying on Bayview to safeguard the PII from unauthorized access, acquisition, and misuse, Lakeview assumed a duty to use reasonable care, including requiring, verifying, and ensuring that Bayview safeguarded the PII of Plaintiffs and Class Members against unauthorized access, acquisition, and misuse.

639. Lakeview failed to use reasonable care by entrusting the PII to Bayview under the following circumstances:

- a. Lakeview did not require, verify, or ensure that the PII of Plaintiffs and Class Members was encrypted.
- b. Lakeview did not require, verify, or ensure that the PII of Plaintiffs and Class Members that Defendants had no reasonable need to store in an internet-accessible environment, including the PII of Plaintiffs and Class Members with whom Lakeview had not had a relationship for years, was not removed from Defendants' network.
- c. Lakeview did not require, verify, or ensure that the movement of the PII of Plaintiffs and Class Members from Defendants' network to the internet was monitored and detected in real time.

- d. Lakeview failed to encrypt the data in its own possession.
- e. Lakeview did not require, verify, or ensure that Bayview included CobaltStrike on the emergency threat feed or tested its “use cases,” allowing the threat attacker to remain on Defendants’ network undetected.
- f. Lakeview did not require, verify, or ensure that Sentinel One—the all-important threat detection and response tool—was feeding into Bayview’s SIEM System.

640. Under like circumstances, a reasonably careful person would have done the following:

- a. Required, verified, and ensured that the PII was encrypted.
- b. Required, verified, and ensured that the PII that Defendants had no reasonable need to store in an internet-accessible environment, including PII of Plaintiffs and Class Members with whom Lakeview had not had a relationship for years, was removed from Defendants’ network.
- c. Required, verified, and ensured that the movement of the PII of Plaintiffs and Class Members from Defendants’ network to the internet was monitored and detected in real time.
- d. Required, verified, and ensured that Bayview included CobaltStrike on the emergency threat feed or tested its “use cases,” thereby preventing the threat attacker from remaining on Defendants’ network undetected.
- e. Required, verified, and ensured that Sentinel One—the all-important threat detection and response tool—was feeding into Bayview’s SIEM System.

641. Lakeview's conduct also constituted negligence per se. As stated herein, Lakeview is a financial institution subject to the requirements of the GLBA, 15 U.S.C. § 6801, *et seq.*, and the FTC Act, 15 U.S.C. § 41, *et seq.* The GLBA required Lakeview to take several preventative security measures to protect Plaintiffs' and Class Members' data, including:

- a. maintaining an adequate data security system to reduce the risk of data breaches and cyber attacks;
- b. adequately protecting Plaintiffs' and Class Members' PII;
- c. implementing policies and procedures to prevent, detect, contain, and correct security violations;
- d. implementing procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports;
- e. protecting against any reasonably anticipated threats or hazards to the security or integrity of PII; and
- f. effectively training all members of their workforce on the policies and procedures with respect to PII as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of PII.

642. By failing to take the above security measures, Lakeview breached duties imposed under federal law, rules, and regulations.

643. Lakeview's negligence directly and in natural and continuous sequence produced or contributed substantially to producing Plaintiffs' and Class Members' damage because of the following:

- a. Lakeview's failure to require, verify, and ensure that Bayview encrypted the PII of Plaintiffs and Class Members allowed the threat attacker to acquire their PII.
- b. Lakeview's failure to require, verify, and ensure that Bayview removed from Defendants' network the PII of Plaintiffs and Class Members that Defendants had no reasonable need to store in an internet-accessible environment, including the PII of Plaintiffs and Class Members with whom Defendants had not had a relationship for years, allowed the threat attacker to acquire their PII.
- c. Lakeview's failure to require, verify, and ensure that Bayview monitored in real time the movement of the PII of Plaintiffs and Class Members from Defendants' network to the internet allowed the threat attacker to exfiltrate the PII without detection and therefore without any attempt to halt the exfiltration before its completion.
- d. Lakeview's failure to require, verify, and ensure that Bayview included CobaltStrike on the emergency threat feed or tested its "use cases," allowed the threat attacker to remain on the network undetected.
- e. Lakeview's failure to require, verify, and ensure that Bayview ensured Sentinel One was feeding into Bayview's SIEM system impeded the detection of CobaltStrike activity.
- f. Lakeview's failure to encrypt the data in its own possession.

644. But for Lakeview's negligence, the damage to Plaintiffs and Class Members would not have occurred because of the following:

- a. If Lakeview had required, verified, and ensured encryption of the PII of Plaintiff and Class Members, the threat attacker would not have acquired their PII.
- b. If Lakeview had required, verified, and ensured that Bayview removed from Defendants' network the PII of Plaintiffs and Class Members that Defendants had no reasonable need to store in an internet-accessible environment, the threat attacker would not have acquired their PII.
- c. If Lakeview had required, verified, and ensured that Bayview monitored in real time the movement of the PII of Plaintiffs and Class Members from Defendants' network to the internet, the exfiltration of the PII could have been halted before its completion.
- d. If Lakeview had required, verified, and ensured that Bayview had included CobaltStrike on the emergency threat feed or tested its "use cases," the threat attacker would have been prevented from remaining on the network undetected.
- e. If Lakeview had required, verified, and ensured that Bayview ensured Sentinel One was feeding into Bayview's SIEM, the CobaltStrike activity would have been detected.

645. Lakeview's negligence was a legal cause of damage to Plaintiffs and Class Members, even if it operated in combination with the acts of the threat attacker, because the acts of and the harm caused by the threat attacker were reasonably foreseeable, and Lakeview's negligence contributed substantially to producing such damage to Plaintiffs and Class Members.

Community Loan—Duty, Breach, and Causation

646. Prior to the Data Breach, Community Loan knowingly and intentionally acquired the PII of Plaintiffs and Class Members, including their Social Security numbers, either directly or indirectly from Plaintiffs and Class Members.

647. In knowingly and intentionally entrusting the PII of Plaintiffs and Class Members to Bayview and relying on Bayview to safeguard the PII from unauthorized access, acquisition, and misuse, Community Loan assumed a duty to use reasonable care, including requiring, verifying, and ensuring that Bayview safeguarded the PII of Plaintiffs and Class Members against unauthorized access, acquisition, and misuse.

648. Community Loan failed to use reasonable care by entrusting the PII to Bayview under the following circumstances:

- a. Community Loan did not require, verify, or ensure that the PII of Plaintiffs and Class Members was encrypted.
- b. Community Loan did not require, verify, or ensure that the PII of Plaintiffs and Class Members that Defendants had no reasonable need to store in an internet-accessible environment, including the PII of Plaintiffs and Class Members with whom Community Loan had not had a relationship for years, was not removed from Defendants' network.
- c. Community Loan did not require, verify, or ensure that the movement of the PII of Plaintiffs and Class Members from Defendants' network to the internet was monitored and detected in real time.
- d. Community Loan failed to encrypt the data in its own possession.

- e. Community Loan did not require, verify, or ensure that Bayview included CobaltStrike on the emergency threat feed or tested its “use cases,” allowing the threat attacker to remain on Defendants’ network undetected.
- f. Community Loan did not require, verify, or ensure that Sentinel One—the all-important threat detection and response tool—was feeding into Bayview’s SIEM System.

649. Under like circumstances, a reasonably careful person would have done the following:

- a. Required, verified, and ensured that the PII was encrypted.
- b. Required, verified, and ensured that the PII that Defendants had no reasonable need to store in an internet-accessible environment, including PII of Plaintiffs and Class Members with whom Community Loan had not had a relationship for years, was removed from Defendants’ network.
- c. Required, verified, and ensured that the movement of the PII of Plaintiffs and Class Members from Defendants’ network to the internet was monitored and detected in real time.
- d. Required, verified, and ensured that Bayview included CobaltStrike on the emergency threat feed or tested its “use cases,” thereby preventing the threat attacker from remaining on Defendants’ network undetected.
- e. Required, verified, and ensured that Sentinel One—the all-important threat detection and response tool—was feeding into Bayview’s SIEM System.

650. Community Loan’s conduct also constituted negligence per se. As stated herein, Community Loan is a financial institution subject to the requirements of the GLBA, 15 U.S.C. §

6801, *et seq.*, and the FTC Act, 15 U.S.C. § 41, *et seq.* The GLBA required Community Loan to take several preventative security measures to protect Plaintiffs' and Class Members' data, including:

- a. maintaining an adequate data security system to reduce the risk of data breaches and cyber attacks;
- b. adequately protecting Plaintiffs' and Class Members' PII;
- c. implementing policies and procedures to prevent, detect, contain, and correct security violations;
- d. implementing procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports;
- e. protecting against any reasonably anticipated threats or hazards to the security or integrity of PII; and
- f. effectively training all members of their workforce on the policies and procedures with respect to PII as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of PII.

651. By failing to take the above security measures, Community Loan breached duties imposed under federal law, rules, and regulations.

652. Community Loan's negligence directly and in natural and continuous sequence produced or contributed substantially to producing Plaintiffs' and Class Members' damage because of the following:

- a. Community Loan's failure to require, verify, and ensure that Bayview encrypted the PII of Plaintiffs and Class Members allowed the threat attacker to acquire their PII.

- b. Community Loan's failure to require, verify, and ensure that Bayview removed from Defendants' network the PII of Plaintiffs and Class Members that Defendants had no reasonable need to store in an internet-accessible environment, including the PII of Plaintiffs and Class Members with whom Defendants had not had a relationship for years, allowed the threat attacker to acquire their PII.
- c. Community Loan's failure to require, verify, and ensure that Bayview monitored in real time the movement of the PII of Plaintiffs and Class Members from Defendants' network to the internet allowed the threat attacker to exfiltrate the PII without detection and therefore without any attempt to halt the exfiltration before its completion.
- d. Community Loan's failure to require, verify, and ensure that Bayview included CobaltStrike on the emergency threat feed or tested its "use cases," allowed the threat attacker to remain on the network undetected.
- e. Community Loan's failure to require, verify, and ensure that Bayview ensured Sentinel One was feeding into Bayview's SIEM system impeded the detection of CobaltStrike activity.
- f. Community Loan's failure to encrypt the data in its own possession.

653. But for Community Loan's negligence, the damage to Plaintiffs and Class Members would not have occurred because of the following:

- a. If Community Loan had required, verified, and ensured encryption of the PII of Plaintiff and Class Members, the threat attacker would not have acquired their PII.

- b. If Community Loan had required, verified, and ensured that Bayview removed from Defendants' network the PII of Plaintiffs and Class Members that Defendants had no reasonable need to store in an internet-accessible environment, the threat attacker would not have acquired their PII.
- c. If Community Loan had required, verified, and ensured that Bayview monitored in real time the movement of the PII of Plaintiffs and Class Members from Defendants' network to the internet, the exfiltration of the PII could have been halted before its completion.
- d. If Community Loan had required, verified, and ensured that Bayview had included CobaltStrike on the emergency threat feed or tested its "use cases," the threat attacker would have been prevented from remaining on the network undetected.
- e. If Community Loan had required, verified, and ensured that Bayview ensured Sentinel One was feeding into Bayview's SIEM, the CobaltStrike activity would have been detected.

654. Community Loan's negligence was a legal cause of damage to Plaintiffs and Class Members, even if it operated in combination with the acts of the threat attacker, because the acts of and the harmed caused by the threat attacker were reasonably foreseeable, and Community Loan's negligence contributed substantially to producing such damage to Plaintiffs and Class Members.

Pingora—Duty, Breach, and Causation

655. Prior to the Data Breach, Pingora knowingly and intentionally acquired the PII of Plaintiffs and Class Members, including their Social Security numbers, either directly or indirectly from Plaintiffs and Class Members.

656. In knowingly and intentionally entrusting the PII of Plaintiffs and Class Members to Bayview and relying on Bayview to safeguard the PII from unauthorized access, acquisition, and misuse, Pingora assumed a duty to use reasonable care, including requiring, verifying, and ensuring that Bayview safeguarded the PII of Plaintiffs and Class Members against unauthorized access, acquisition, and misuse.

657. Pingora failed to use reasonable care by entrusting the PII to Bayview under the following circumstances:

- a. Pingora did not require, verify, or ensure that the PII of Plaintiffs and Class Members was encrypted.
- b. Pingora did not require, verify, or ensure that the PII of Plaintiffs and Class Members that Defendants had no reasonable need to store in an internet-accessible environment, including the PII of Plaintiffs and Class Members with whom Pingora had not had a relationship for years, was not removed from Defendants' network.
- c. Pingora did not require, verify, or ensure that the movement of the PII of Plaintiffs and Class Members from Defendants' network to the internet was monitored and detected in real time.
- d. Pingora failed to encrypt the data in its own possession.

- e. Pingora did not require, verify, or ensure that Bayview included CobaltStrike on the emergency threat feed or tested its “use cases,” allowing the threat attacker to remain on Defendants’ network undetected.
- f. Pingora did not require, verify, or ensure that Sentinel One—the all-important threat detection and response tool—was feeding into Bayview’s SIEM System.

658. Under like circumstances, a reasonably careful person would have done the following:

- a. Required, verified, and ensured that the PII was encrypted.
- b. Required, verified, and ensured that the PII that Defendants had no reasonable need to store in an internet-accessible environment, including PII of Plaintiffs and Class Members with whom Pingora had not had a relationship for years, was removed from Defendants’ network.
- c. Required, verified, and ensured that the movement of the PII of Plaintiffs and Class Members from Defendants’ network to the internet was monitored and detected in real time.
- d. Required, verified, and ensured that Bayview included CobaltStrike on the emergency threat feed or tested its “use cases,” thereby preventing the threat attacker from remaining on Defendants’ network undetected.
- e. Required, verified, and ensured that Sentinel One—the all-important threat detection and response tool—was feeding into Bayview’s SIEM System.

659. Pingora’s conduct also constituted negligence per se. As stated herein, Pingora is a financial institution subject to the requirements of the GLBA, 15 U.S.C. § 6801, *et seq.*, and the

FTC Act, 15 U.S.C. § 41, *et seq.* The GLBA required Pingora to take several preventative security measures to protect Plaintiffs' and Class Members' data, including:

- a. maintaining an adequate data security system to reduce the risk of data breaches and cyber attacks;
- b. adequately protecting Plaintiffs' and Class Members' PII;
- c. implementing policies and procedures to prevent, detect, contain, and correct security violations;
- d. implementing procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports;
- e. protecting against any reasonably anticipated threats or hazards to the security or integrity of PII; and
- f. effectively training all members of their workforce on the policies and procedures with respect to PII as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of PII.

660. By failing to take the above security measures, Pingora breached duties imposed under federal law, rules, and regulations.

661. Pingora's negligence directly and in natural and continuous sequence produced or contributed substantially to producing Plaintiffs' and Class Members' damage because of the following:

- a. Pingora's failure to require, verify, and ensure that Bayview encrypted the PII of Plaintiffs and Class Members allowed the threat attacker to acquire their PII.
- b. Pingora's failure to require, verify, and ensure that Bayview removed from Defendants' network the PII of Plaintiffs and Class Members that Defendants

had no reasonable need to store in an internet-accessible environment, including the PII of Plaintiffs and Class Members with whom Defendants had not had a relationship for years, allowed the threat attacker to acquire their PII.

- c. Pingora's failure to require, verify, and ensure that Bayview monitored in real time the movement of the PII of Plaintiffs and Class Members from Defendants' network to the internet allowed the threat attacker to exfiltrate the PII without detection and therefore without any attempt to halt the exfiltration before its completion.
- d. Pingora's failure to require, verify, and ensure that Bayview included CobaltStrike on the emergency threat feed or tested its "use cases," allowed the threat attacker to remain on the network undetected.
- e. Pingora's failure to require, verify, and ensure that Bayview ensured Sentinel One was feeding into Bayview's SIEM system impeded the detection of CobaltStrike activity.
- f. Pingora's failure to encrypt the data in its own possession.

662. But for Pingora's negligence, the damage to Plaintiffs and Class Members would not have occurred because of the following:

- a. If Pingora had required, verified, and ensured encryption of the PII of Plaintiff and Class Members, the threat attacker would not have acquired their PII.
- b. If Pingora had required, verified, and ensured that Bayview removed from Defendants' network the PII of Plaintiffs and Class Members that Defendants had no reasonable need to store in an internet-accessible environment, the threat attacker would not have acquired their PII.

- c. If Pingora had required, verified, and ensured that Bayview monitored in real time the movement of the PII of Plaintiffs and Class Members from Defendants' network to the internet, the exfiltration of the PII could have been halted before its completion.
- d. If Pingora had required, verified, and ensured that Bayview had included CobaltStrike on the emergency threat feed or tested its "use cases," the threat attacker would have been prevented from remaining on the network undetected.
- e. If Pingora had required, verified, and ensured that Bayview ensured Sentinel One was feeding into Bayview's SIEM, the CobaltStrike activity would have been detected.

663. Pingora's negligence was a legal cause of damage to Plaintiffs and Class Members, even if it operated in combination with the acts of the threat attacker, because the acts of and the harmed caused by the threat attacker were reasonably foreseeable, and Pingora's negligence contributed substantially to producing such damage to Plaintiffs and Class Members.

Damages

664. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft, including unauthorized charges; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII, including the exposure of their PII on the dark web and the substantial risk of future harm; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes; (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 present and continuing 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; (viii) damages consisting of the cost of identity theft protection services for the remainder of the lives of Plaintiffs and Class Members; and (ix) 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 resulting from the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

665. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered and will suffer the continued risk 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.

666. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members are now at an increased risk of identity theft or fraud.

667. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members are entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT II
BREACH OF CONTRACT (THIRD-PARTY BENEFICIARY)
On behalf of All Plaintiffs and the Class or, Alternatively, the Subclasses
Against Lakeview, Community Loan, and Pingora

668. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 625.

Lakeview

669. Lakeview entered into written contracts with various financial institutions and entities from which it obtained the PII of Plaintiffs and Class Members.

670. Lakeview and these entities intended that Plaintiffs and Class Members, as borrowers required to provide their confidential PII, benefit from these contracts.

671. The contracts required Lakeview to safeguard the PII of Plaintiffs and Class Members, including as follows:

- a. The contracts required Lakeview to acknowledge that all non-public personal information of a consumer or customer of the other party which was made available to Lakeview in connection with the contracts, or which became available to Lakeview in connection with the contracts, was to be protected by Lakeview from unauthorized use and disclosure.
- b. The contracts required Lakeview to take all reasonable measures, including without limitation such measures as it takes to safeguard its own confidential information, to ensure the security and confidentiality of all information provided to it by the other party, to protect against all threats or hazards to the security or integrity of the information, and to protect against unauthorized access to or use of the information.

- c. The contracts required Lakeview to maintain an information security program that includes administrative, technical and physical safeguards designed to protect the security and confidentiality of the confidential information disclosed by the other party.
- d. The contracts required Lakeview to conduct testing for vulnerability and penetration of its computer systems in accordance with industry standards.
- e. The contracts required Lakeview to meet or exceed industry standards as a means to protect any information concerning consumers and to prevent any compromise of Lakeview's information systems, computer networks or data files.

672. The circumstances under which the contracts were entered include the following:

- a. The other parties to the contracts needed a servicer for loans issued to Plaintiffs and Class Members.
- b. The other parties to the contracts intended to entrust the PII of Plaintiffs and Class Members to Lakeview and sought assurance that Lakeview would safeguard their PII.

673. The apparent purposes the parties to the contracts were trying to accomplish included the following:

- a. Obtain and provide servicing of loans issued to Plaintiffs and Class Members.
- b. Ensure that Lakeview safeguarded the PII of Plaintiffs and Class Members.

674. Lakeview breached the contracts as follows:

- a. Failing to require, verify, or ensure that the PII of Plaintiffs and Class Members was encrypted.

- b. Failing to require, verify, or ensure that the PII of Plaintiffs and Class Members that Defendants had no reasonable need to store in an internet-accessible environment, including the PII of Plaintiffs and Class Members with whom Lakeview had not had a relationship for years, was not removed from Defendants' network.
- c. Failing to require, verify, or ensure that the movement of the PII of Plaintiffs and Class Members from Defendants' network to the internet was monitored and detected in real time.
- d. Failing to require, verify, or ensure that Bayview included CobaltStrike on the emergency threat feed or tested its "use cases," allowing the threat attacker to remain on Defendants' network undetected.
- e. Failing to require, verify, or ensure that Sentinel One—the all-important threat detection and response tool—was feeding into Bayview's SIEM System.

675. Lakeview's breaches of the contracts caused the PII of Plaintiffs and Class Members to be acquired by the threat actor and misused as a result of that acquisition.

676. But for Lakeview's breaches of the contracts, the PII of Plaintiffs and Class Members would not have been acquired by the threat actor and misused as a result of that acquisition.

Community Loan

677. Community Loan entered into written contracts with various financial institutions and entities from which it obtained the PII of Plaintiffs and Class Members.

678. Community Loan and these entities intended that Plaintiffs and Class Members, as borrowers required to provide their confidential PII, benefit from these contracts.

679. The contracts required Community Loan to safeguard the PII of Plaintiffs and Class Members, including as follows:

- a. The contracts required Community Loan to acknowledge that all non-public personal information of a consumer or customer of the other party which was made available to Community Loan in connection with the contracts, or which became available to Community Loan in connection with the contracts, was to be protected by Community Loan from unauthorized use and disclosure.
- b. The contracts required Community Loan to take all reasonable measures, including without limitation such measures as it takes to safeguard its own confidential information, to ensure the security and confidentiality of all information provided to it by the other party, to protect against all threats or hazards to the security or integrity of the information, and to protect against unauthorized access to or use of the information.
- c. The contracts required Community Loan to maintain an information security program that includes administrative, technical and physical safeguards designed to protect the security and confidentiality of the confidential information disclosed by the other party.
- d. The contracts required Community Loan to conduct testing for vulnerability and penetration of its computer systems in accordance with industry standards.
- e. The contracts required Community Loan to meet or exceed industry standards as a means to protect any information concerning consumers and to prevent any compromise of Community Loan's information systems, computer networks or data files.

680. The circumstances under which the contracts were entered include the following:

- a. The other parties to the contracts needed a servicer for loans issued to Plaintiffs and Class Members.
- b. The other parties to the contracts intended to entrust the PII of Plaintiffs and Class Members to Community Loan and sought assurance that Community Loan would safeguard their PII.

681. The apparent purposes the parties to the contracts were trying to accomplish included the following:

- a. Obtain and provide servicing of loans issued to Plaintiffs and Class Members.
- b. Ensure that Community Loan safeguarded the PII of Plaintiffs and Class Members.

682. Community Loan breached the contracts as follows:

- a. Failing to require, verify, or ensure that the PII of Plaintiffs and Class Members was encrypted.
- b. Failing to require, verify, or ensure that the PII of Plaintiffs and Class Members that Defendants had no reasonable need to store in an internet-accessible environment, including the PII of Plaintiffs and Class Members with whom Community Loan had not had a relationship for years, was not removed from Defendants' network.
- c. Failing to require, verify, or ensure that the movement of the PII of Plaintiffs and Class Members from Defendants' network to the internet was monitored and detected in real time.

- d. Failing to require, verify, or ensure that Bayview included CobaltStrike on the emergency threat feed or tested its “use cases,” allowing the threat attacker to remain on Defendants’ network undetected.

683. Failing to require, verify, or ensure that Sentinel One—the all-important threat detection and response tool—was feeding into Bayview’s SIEM System.

684. Community Loan’s breaches of the contracts caused the PII of Plaintiffs and Class Members to be acquired by the threat actor and misused as a result of that acquisition.

685. But for Community Loan’s breaches of the contracts, the PII of Plaintiffs and Class Members would not have been acquired by the threat actor and misused as a result of that acquisition.

Pingora

686. Pingora entered into written contracts with various financial institutions and entities from which it obtained the PII of Plaintiffs and Class Members.

687. Pingora and these entities intended that Plaintiffs and Class Members, as borrowers required to provide their confidential PII, benefit from these contracts.

688. The contracts required Pingora to safeguard the PII of Plaintiffs and Class Members, including as follows:

- a. The contracts required Pingora to acknowledge that all non-public personal information of a consumer or customer of the other party which was made available to Pingora in connection with the contracts, or which became available to Pingora in connection with the contracts, was to be protected by Pingora from unauthorized use and disclosure.

- b. The contracts required Pingora to take all reasonable measures, including without limitation such measures as it takes to safeguard its own confidential information, to ensure the security and confidentiality of all information provided to it by the other party, to protect against all threats or hazards to the security or integrity of the information, and to protect against unauthorized access to or use of the information.
- c. The contracts required Pingora to maintain an information security program that includes administrative, technical and physical safeguards designed to protect the security and confidentiality of the confidential information disclosed by the other party.
- d. The contracts required Pingora to conduct testing for vulnerability and penetration of its computer systems in accordance with industry standards.
- e. The contracts required Pingora to meet or exceed industry standards as a means to protect any information concerning consumers and to prevent any compromise of Pingora's information systems, computer networks or data files.

689. The circumstances under which the contracts were entered include the following:

- a. The other parties to the contracts needed a servicer for loans issued to Plaintiffs and Class Members.
- b. The other parties to the contracts intended to entrust the PII of Plaintiffs and Class Members to Pingora and sought assurance that Pingora would safeguard their PII.

690. The apparent purposes the parties to the contracts were trying to accomplish included the following:

- a. Obtain and provide servicing of loans issued to Plaintiffs and Class Members.
- b. Ensure that Pingora safeguarded the PII of Plaintiffs and Class Members.

691. Pingora breached the contracts as follows:

- a. Failing to require, verify, or ensure that the PII of Plaintiffs and Class Members was encrypted.
- b. Failing to require, verify, or ensure that the PII of Plaintiffs and Class Members that Defendants had no reasonable need to store in an internet-accessible environment, including the PII of Plaintiffs and Class Members with whom Pingora had not had a relationship for years, was not removed from Defendants' network.
- c. Failing to require, verify, or ensure that the movement of the PII of Plaintiffs and Class Members from Defendants' network to the internet was monitored and detected in real time.
- d. Failing to require, verify, or ensure that Bayview included CobaltStrike on the emergency threat feed or tested its "use cases," allowing the threat attacker to remain on Defendants' network undetected.

692. Failing to require, verify, or ensure that Sentinel One—the all-important threat detection and response tool—was feeding into Bayview's SIEM System.

693. Pingora's breaches of the contracts caused the PII of Plaintiffs and Class Members to be acquired by the threat actor and misused as a result of that acquisition.

694. But for Pingora's breaches of the contracts, the PII of Plaintiffs and Class Members would not have been acquired by the threat actor and misused as a result of that acquisition.

Damages

695. As a direct and proximate result of Lakeview's, Community Loan's, and Pingora's above-described breaches, Plaintiffs and Class Members 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; damages consisting of the cost of identity theft protection services for the remainder of the lives of Plaintiffs and Class Members; additional time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts and credit freezes; decreased credit scores and ratings; lost work time; and other economic and non-economic harm including 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 resulting from the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

696. As a direct and proximate result of Lakeview's, Community Loan's, and Pingora's breaches of contract, Plaintiffs and Class Members are at an increased risk of identity theft or fraud.

697. As a direct and proximate result of Lakeview's, Community Loan's, and Pingora's breaches of contract, Plaintiffs and Class Members are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

COUNT III
VIOLATIONS OF CALIFORNIA’S CONSUMER PRIVACY ACT,
Cal. Civ. Code § 1798.100, *et seq.* (2020) (“CCPA”)¹⁴⁴
On Behalf of Plaintiffs Robert Keach, Cindy Villanueva, Pedro Rubio, Norma Grossman,
Maureen Keach, Linda Kim, and Jay Saporta and the California Subclass
Against All Defendants

698. Plaintiffs Robert Keach, Cindy Villanueva, Pedro Rubio, Norma Grossman, Maureen Keach, Linda Kim, and Jay Saporta (“Plaintiffs,” for purposes of this Count) and the California Subclass re-allege and incorporate paragraphs 1 through 625 as if fully set forth herein.

699. Plaintiffs Cindy Villanueva and Pedro Rubio bring this claim on behalf of themselves and the California Subclass against Defendants Bayview and Lakeview.

700. Plaintiffs Robert Keach, Maureen Keach, Norma Grossman, and Jay Saporta bring this claim on behalf of themselves and the California Subclass against Defendants Bayview and Pingora.

701. Plaintiff Linda Kim brings this claim on behalf of herself and the California Subclass against Defendants Bayview and Community Loan.

702. Section 1798.150(a)(1) of the CCPA provides, “[a]ny consumer whose nonencrypted or nonredacted personal information, as defined by [Cal. Civ. Code section 1798.81.5(d)(1)(A)] . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for” statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

¹⁴⁴ The CCPA went into effect in 2020 and was amended in 2023. Plaintiffs’ citations herein are to the 2020 version, which was the operative version of the statute, to which Defendants were subject, when the Data Breach occurred.

703. Plaintiffs and the California Subclass Members are consumers and California residents as defined by Cal. Civ. Code section 1798.140(g).

Bayview

704. Bayview is a “business” as defined by Cal. Civ. Code § 1798.140(c)(1) because it is a “sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers’ personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information, that does business in the State of California . . . [and] [h]as annual gross revenues in excess of twenty-five million dollars (\$25,000,000) . . . [and] alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.”¹⁴⁵

705. Bayview collects personal information from, among other sources, consumers whose loans are serviced by Bayview and by its affiliated companies Pingora, Lakeview, and Community Loan.

706. Bayview, Pingora, Lakeview, and Community Loan jointly determine the purposes and means of processing consumers’ personal information. Lakeview, Community Loan, and Pingora obtain personal information from their customers for the purpose of servicing their loans. In turn, Lakeview, Community Loan, and Pingora share this personal information with their parent company, Bayview, which in coordination with Lakeview, Community Loan, and Pingora, assists

¹⁴⁵

https://rocketreach.co/bayview-asset-management-llc-profile_b5c2a8a1f42e0f27#:~:text=What%20is%20the%20annual%20revenue,was%20%24928%20million%20in%202023 (last visited Jan. 16, 2024).

with the technical aspects of processing and storing the information so that it can be used by all of these entities to service loans and manage portfolios of mortgages.

707. Bayview provides data security and storage services for the personal information obtained from the customers of its subsidiaries Lakeview, Community Loan, and Pingora. Bayview, Lakeview, Community Loan, and Pingora regularly communicate and work together to determine how this personal information is processed, including through implementation of software and other technical updates, and the purposes—including loan servicing and mortgage portfolio management—for which this information is used. Hence, Bayview, Lakeview, Community Loan, and Pingora jointly determined both the purpose and the means of processing Plaintiffs' data.

708. Plaintiffs' and California Subclass Members' personal information, as defined by Civil Code section 1798.140(o), was subject to unauthorized access and exfiltration, theft, or disclosure. The Data Breach described herein exposed, without limitation, names, addresses, loan numbers, Social Security numbers, and, for some California Subclass Members, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

709. Bayview 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.

710. Bayview failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect PII by:

- a. failing to encrypt the PII of Plaintiffs and California Subclass Members;

- b. failing to delete the PII of Plaintiffs and Class Members after it was no longer necessary to retain the PII;
- c. storing Plaintiffs' and California Subclass Members' PII in an internet-accessible environment when such storage was unnecessary;
- d. continuing to accept and store PII after it knew or should have known about the Data Breach;
- e. failing to monitor and detect the movement of the PII of Plaintiffs and California Subclass Members from Bayview's network to the internet in real time;
- f. failing to monitor the practices of its cybersecurity vendors;
- g. failing to include CobaltStrike—the software the attackers used—on the emergency threat feed or test its “use cases,” allowing the threat attacker to remain on Bayview's network undetected;
- h. failing to properly integrate Sentinel One—the all-important threat detection and response tool—into Bayview's Security Information and Events Management System; and
- i. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiffs and California Subclass Members from taking timely self-protection measures.

711. The Data Breach occurred as a result of Bayview's failure to implement and maintain reasonable security procedures and practices for protecting the exposed information given its nature. Bayview also failed to monitor its systems to identify suspicious activity, and allowed unauthorized access to Plaintiffs' and California Subclass Members' PII.

712. Bayview violated section 1798.150(a) of the CCPA, Cal. Civ. Code § 1798.150(a), by failing to prevent Plaintiffs’ and California Subclass Members’ PII from unauthorized access, exfiltration, theft, or disclosure as a result of Bayview’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.

713. Plaintiffs and the California Subclass Members suffered damage and losses as a direct and proximate result of Bayview’s conduct described above.

Lakeview

714. Lakeview is a “business” as defined by Cal. Civ. Code § 1798.140(c)(1) because it is a “sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers’ personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information, that does business in the State of California . . . [and] [h]as annual gross revenues in excess of twenty-five million dollars (\$25,000,000) . . . [and] alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.”¹⁴⁶

715. Lakeview collects personal information from, among other sources, the consumers whose loans are serviced by Lakeview and its affiliated companies: Bayview, Pingora, and Community Loan.

¹⁴⁶ <https://www.zoominfo.com/c/lakeview-loan-servicing-llc/354955782> (last visited Jan. 16, 2024).

716. Lakeview, Bayview, Pingora, and Community Loan jointly determine the purposes and means of processing consumers' personal information. Lakeview, Community Loan, and Pingora obtain personal information from their customers for the purpose of servicing their loans. In turn, Lakeview, Community Loan, and Pingora share this personal information with their parent company, Bayview, which in coordination with Lakeview, Community Loan, and Pingora, assists with the technical aspects of processing and storing the information so that it can be used by all of these entities to service loans and manage portfolios of mortgages.

717. Bayview provides data security and storage services for the personal information obtained from the customers of its subsidiaries Lakeview, Community Loan, and Pingora. Lakeview, Bayview, Community Loan, and Pingora regularly communicate and work together to determine how this personal information is processed, including through implementation of software and other technical updates, and the purposes—including loan servicing and mortgage portfolio management—for which this information is used. For example, the Chief Compliance Officers from Bayview, Lakeview, Community Loan, and Pingora all [REDACTED]

[REDACTED]

[REDACTED].¹⁴⁸ Hence, Lakeview, Bayview, Community Loan, and Pingora jointly determined both the purpose and the means of processing Plaintiffs' data.

718. Plaintiffs' and California Subclass Members' personal information, as defined by Civil Code section 1798.140(o), was subject to unauthorized access, exfiltration, theft, or disclosure. The Data Breach described herein exposed, without limitation, name, address, loan

¹⁴⁷ BAYVIEW000147258 at 7261.

¹⁴⁸ BAYVIEW000122966.

number, and Social Security number, and, for some California Subclass Members, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

719. Lakeview 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.

720. Lakeview failed to implement and maintain reasonable security procedures by:

- a. failing to require, verify, or ensure that the PII of Plaintiffs and California Subclass Members was encrypted;
- b. failing to delete the PII of Plaintiffs and California Subclass Members after it was no longer necessary to retain the PII;
- c. storing Plaintiffs' and California Subclass Members' PII in an internet-accessible environment when such storage was unnecessary;
- d. continuing to accept and store PII after it knew or should have known of the Data Breach;
- e. failing to monitor the cybersecurity practices of Bayview;
- f. failing to monitor the practices of its cybersecurity vendors; and
- g. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiffs and California Subclass Members from taking timely self-protection measures.

721. The Data Breach occurred as a result of Lakeview's failure to implement and maintain reasonable security procedures and practices for protecting the exposed information

given its nature. Lakeview failed to monitor its systems to identify suspicious activity, and allowed unauthorized access to Plaintiffs' and California Subclass Members' PII.

722. Lakeview violated section 1798.150(a) of the CCPA, Cal. Civ. Code § 1798.150(a), by failing to prevent Plaintiffs' and the California Subclass Members' PII from unauthorized access, exfiltration, theft, or disclosure as a result of Lakeview'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.

723. Plaintiffs and the California Subclass Members suffered damage and losses as a direct and proximate result of Lakeview's conduct described above.

Community Loan

724. Community Loan is a "business" as defined by Cal. Civ. Code § 1798.140(c)(1) because it is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California . . . [and] [h]as annual gross revenues in excess of twenty-five million dollars (\$25,000,000) . . . [and] alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices."¹⁴⁹

¹⁴⁹ Community Loan Servicing, ZOOMINFO, <https://www.zoominfo.com/c/community-loan-servicing-llc/527507430> (last visited Jan. 16, 2024).

725. Community Loan collects personal information from, among other sources, the consumers whose loans are serviced by Community Loan and its affiliated companies: Pingora, Lakeview, and Bayview.

726. Community Loan, Bayview, Pingora, and Lakeview jointly determine the purposes and means of processing consumers' personal information. Community Loan, Lakeview, and Pingora obtain personal information from their customers for the purpose of servicing their loans. In turn, Community Loan, Lakeview, and Pingora share this personal information with their parent company, Bayview, which in coordination with Community Loan, Lakeview, and Pingora, assists with the technical aspects of processing and storing the information so that it can be used by all of these entities to service loans and manage portfolios of mortgages.

727. Bayview provides data security and storage services for the personal information obtained from the customers of its subsidiaries Community Loan, Lakeview, and Pingora. Community Loan, Bayview, Lakeview, and Pingora regularly communicate and work together to determine how this personal information is processed, including through implementation of software and other technical updates, and the purposes—including loan servicing and mortgage portfolio management—for which this information is used. For example, the Chief Compliance Officers from Bayview, Lakeview, Community Loan, and Pingora all [REDACTED]

[REDACTED]

[REDACTED].¹⁵¹ Hence, Lakeview, Bayview, Community Loan, and Pingora jointly determined both the purpose and the means of processing Plaintiffs' data.

¹⁵⁰ BAYVIEW000147258 at 7261.

¹⁵¹ BAYVIEW000122966.

728. Plaintiffs' and California Subclass Members' personal information, as defined by Civil Code section 1798.140(o), was subject to unauthorized access, exfiltration, theft, or disclosure. The Data Breach described herein exposed, without limitation, name, address, loan number, and Social Security number, and, for some California Subclass Members, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

729. Community Loan 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.

730. Community Loan failed to implement and maintain reasonable security procedures by:

- a. failing to require, verify, or ensure that the PII of Plaintiffs and California Subclass Members was encrypted;
- b. failing to delete the PII of Plaintiffs and California Subclass Members after it was no longer necessary to retain the PII;
- c. storing Plaintiffs' and California Subclass Members' PII in an internet-accessible environment when such storage was unnecessary;
- d. continuing to accept and store PII after it knew or should have known of the Data Breach;
- e. failing to monitor the cybersecurity practices of Bayview;
- f. failing to monitor the practices of its cybersecurity vendors; and

- g. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiffs and California Subclass Members from taking timely self-protection measures.

731. The Data Breach occurred as a result of Community Loan's failure to implement and maintain reasonable security procedures and practices for protecting the exposed information given its nature. Community Loan also failed to monitor its systems to identify suspicious activity, and allowed unauthorized access to Plaintiffs' and California Subclass Members' PII.

732. Community Loan violated section 1798.150(a) of the CCPA, Cal. Civ. Code § 1798.150(a), by failing to prevent Plaintiffs' and the California Subclass Members' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Community Loan'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.

733. Plaintiffs and the California Subclass Members suffered damage and losses as a direct and proximate result of Community Loan's conduct described above.

Pingora

734. Pingora is a "business" as defined by Cal. Civ. Code § 1798.140(c)(1) because it is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California . . . [and it] alone or in combination, annually buys, receives for the business's commercial

purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.”

735. Pingora collects personal information from, among other sources, the consumers whose loans are serviced by Pingora and its affiliated companies: Community Loan, Lakeview, and Bayview.

736. Pingora, Lakeview, Bayview, and Community Loan jointly determine the purposes and means of processing consumers’ personal information. Pingora, Lakeview, and Community Loan obtain personal information from their customers for the purpose of servicing their loans. In turn, Pingora, Lakeview, and Community Loan share this personal information with their parent company, Bayview, which in coordination with Pingora, Lakeview, and Community Loan, assists with the technical aspects of processing and storing the information so that it can be used by all of these entities to service loans and manage portfolios of mortgages.

737. Bayview provides data security and storage services for the personal information obtained from the customers of its subsidiaries Pingora, Lakeview, and Community Loan. Pingora, Lakeview, Bayview, and Community Loan regularly communicate and work together to determine how this personal information is processed, including through implementation of software and other technical updates, and the purposes—including loan servicing and mortgage portfolio management—for which this information is used. For example, the Chief Compliance Officers from Bayview, Lakeview, Community Loan, and Pingora all participate on Bayview’s Enterprise Risk Management Steering Committee.¹⁵² Bayview also hired a third-party consulting company, Protiviti, to map out the locations of data held by Lakeview, Pingora, and Community Loan.¹⁵³

¹⁵² BAYVIEW000147258 at 7261.

¹⁵³ BAYVIEW000122966.

Hence, Lakeview, Bayview, Community Loan, and Pingora jointly determined both the purpose and the means of processing Plaintiffs' data.

738. Plaintiffs' and California Subclass Members' personal information, as defined by Civil Code section 1798.140(o), was subject to unauthorized access, exfiltration, theft, or disclosure. The Data Breach described herein exposed, without limitation, name, address, loan number, and Social Security number, and, for some California Subclass Members, information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

739. Pingora 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.

740. Pingora failed to implement and maintain reasonable security procedures by:

- a. failing to require, verify, or ensure that the PII of Plaintiffs and Class Members was encrypted;
- b. failing to delete the PII of Plaintiffs and Class Members after it was no longer necessary to retain the PII;
- c. storing Plaintiffs' and Class Members' PII in an internet-accessible environment when such storage was unnecessary;
- d. continuing to accept and store PII after it knew or should have known of the Data Breach;
- e. failing to monitor the cybersecurity practices of Bayview;
- f. failing to monitor the practices of its cybersecurity vendors; and

- g. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiffs and Class Members from taking timely self-protection measures.

741. The Data Breach occurred as a result of Pingora's failure to implement and maintain reasonable security procedures and practices for protecting the exposed information given its nature. Pingora failed to monitor its systems to identify suspicious activity, and allowed unauthorized access to Plaintiffs' and California Subclass Members' PII.

742. Pingora violated section 1798.150(a) of the CCPA, Cal. Civ. Code § 1798.150(a), by failing to prevent Plaintiffs' and the California Subclass Members' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Pingora'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.

743. Plaintiffs and the California Subclass Members suffered damage and losses as a direct and proximate result of Pingora's conduct described above.

Entitlement to Statutory Damages and Other Relief

744. In view of the foregoing, Plaintiffs and California Subclass members are entitled to relief under Cal. Civ. Code § 1798.150(a) including, but not limited to, statutory damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty dollars (\$750) per consumer per incident or actual damages, whichever is greater; injunctive or declaratory relief; any other relief the Court deems proper; and attorneys' fees and costs, including as provided under Cal. Code Civ. P. § 1021.5.

Notice of CCPA Violation

745. As detailed in the following paragraphs, each Plaintiff provided the relevant Defendant(s) with written notice of its specific violations of the CCPA, and each Defendant had more than 30 days to cure those violations before the filing of this complaint. Defendants have

[REDACTED]

[REDACTED]

[REDACTED].¹⁵⁴

746. Pursuant to § 1798.150(b) of the CCPA, Plaintiff Robert Keach gave written notice to Defendant Pingora and Bayview of their specific violations of § 1798.150(a) by certified mail dated April 14, 2022.¹⁵⁵ Pingora responded on April 29, 2022 but failed to cure.¹⁵⁶ Bayview did not respond within 30 days as required by the statute and failed to cure.

747. Pursuant to § 1798.150(b) of the CCPA, Plaintiff Cindy Villanueva gave written notice to Defendant Lakeview of its specific violations of § 1798.150(a) by certified mail dated April 29, 2022.¹⁵⁷ Lakeview failed to cure and did not respond within the required 30 days.

748. Pursuant to § 1798.150(b) of the CCPA, Plaintiff Pedro Rubio gave written notice to Defendant Lakeview of its specific violations of § 1798.150(a) by certified mail dated April 13, 2022.¹⁵⁸ Lakeview responded on April 29, 2022 but failed to cure.¹⁵⁹

¹⁵⁴ *E.g.*, Ex. 13 (BAYVIEW000147612-7614).

¹⁵⁵ Ex. 6 (R. Keach, M. Keach, and Saporta CCPA Notice).

¹⁵⁶ Ex. 7 (CCPA Responses).

¹⁵⁷ Ex. 8 (Villanueva CCPA Notice).

¹⁵⁸ Ex. 9 (Rubio CCPA Notice).

¹⁵⁹ Ex. 7 (CCPA Responses).

749. Pursuant to § 1798.150(b) of the CCPA, Plaintiff Norma Grossman gave written notice to Defendant Pingora of its specific violations of § 1798.150(a) by certified mail dated June 6, 2022.¹⁶⁰ Pingora failed to cure and did not respond within the required 30 days.

750. Pursuant to § 1798.150(b) of the CCPA, Plaintiff Maureen Keach gave written notice to Defendants Pingora and Bayview of their specific violations of § 1798.150(a) by certified mail dated April 14, 2022.¹⁶¹ Pingora responded on April 29, 2022 but failed to cure.¹⁶² Bayview failed to cure and did not respond within the required 30 days.

751. Pursuant to § 1798.150(b) of the CCPA, Plaintiff Linda Kim gave written notice to Defendants Bayview and Community Loan of their specific violations of § 1798.150(a) by certified mail dated October 31, 2022.¹⁶³ Bayview and Community Loan responded on November 10, 2022 but failed to cure.¹⁶⁴

752. Pursuant to § 1798.150(b) of the CCPA, Plaintiff Jay Saporta gave written notice to Defendants Bayview and Pingora of their specific violations of § 1798.150(a) by certified mail dated April 14, 2022.¹⁶⁵ Pingora responded on April 29, 2022 but failed to cure.¹⁶⁶ Bayview has not responded.

¹⁶⁰ Ex. 10 (Grossman CCPA Notice).

¹⁶¹ Ex. 6 (R. Keach, M. Keach, and Saporta CCPA Notice).

¹⁶² Ex. 7 (CCPA Responses).

¹⁶³ Ex. 11 (Kim CCPA Notice).

¹⁶⁴ Ex. 7 (CCPA Responses).

¹⁶⁵ Ex. 6 (R. Keach, M. Keach, and Saporta CCPA Notice).

¹⁶⁶ Ex. 7 (CCPA Responses).

COUNT IV
VIOLATION OF CALIFORNIA’S CUSTOMER RECORDS ACT (“CCRA”),
Cal. Civ. Code § 1798.80, *et seq.*
On Behalf of Plaintiffs Robert Keach, Cindy Villanueva, Pedro Rubio, Norma Grossman,
Maureen Keach, Linda Kim, and Jay Saporta and the California Subclass
Against All Defendants

753. Plaintiffs Robert Keach, Cindy Villanueva, Pedro Rubio, Norma Grossman, Maureen Keach, Linda Kim, and Jay Saporta (“Plaintiffs,” for purposes of this Count) and the California Subclass re-allege and incorporate paragraphs 1 through 625 as if fully set forth herein.

754. Plaintiffs Cindy Villanueva and Pedro Rubio bring this claim on behalf of themselves and the California Subclass against Defendants Bayview and Lakeview.

755. Plaintiffs Robert Keach, Maureen Keach, Norma Grossman, and Jay Saporta bring this claim on behalf of themselves and the California Subclass against Defendants Bayview and Pingora.

756. Plaintiff Linda Kim brings this claim on behalf of herself and the California Subclass against Bayview and Community Loan.

757. “[T]o ensure that Personal Information about California residents is protected,” the California Legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that “owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure.”

758. Furthermore, businesses that maintain computerized data that includes PII are required to “notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” Cal. Civ. Code § 1798.82(b). Among other

requirements, the security breach notification must include “the types of Personal Information that were or are reasonably believed to have been the subject of the breach.” Cal. Civ. Code § 1798.82.

759. The Data Breach was a breach of security within the meaning of section 1798.82. PII stolen in the Data Breach, such as name, address, loan number, Social Security number, and other items regarding loan servicing, constitutes “personal information” within the meaning of section 1798.80(e).

760. Plaintiffs and California Subclass Members owned PII that was maintained by Bayview, Lakeview, Community Loan, and/or Pingora and that was the subject of the Data Breach. *See* Cal. Civ. Code § 1798.2.

Bayview

761. Bayview is a business within the meaning of Cal. Civ. Code § 1798.80. Bayview is a corporation organized, chartered, or holding a license or authorization certificate under the laws of Florida.

762. Bayview owns, licenses, or maintains personal information about Californians under Cal. Civ. Code § 1798.81.5(a)(1). Such PII includes, but is not limited to, the first and last names and Social Security numbers of Plaintiffs and the California Subclass Members, along with loan numbers and other information that would permit access to Plaintiffs’ and the California Subclass Members’ financial accounts. *See* Cal. Civ. Code §§ 1798.81.5(d)(1)(A)(i) and (iii).

763. Because Plaintiffs’ and California Subclass Members’ PII was acquired by unauthorized persons during the Data Breach, Bayview had an obligation to disclose the Data Breach immediately following its discovery to the owners or licensees of the PII (*i.e.*, Plaintiffs and the California Subclass Members) as mandated by Cal. Civ. Code § 1798.82.

764. The Data Breach occurred from October 27, 2021 to December 7, 2021, and was discovered by Bayview on December 6, 2021, but Bayview did not disclose the Breach to Class Members until March 16, 2022.¹⁶⁷

765. By failing to disclose the Data Breach immediately following its discovery, Bayview violated Cal. Civ. Code § 1798.82.

766. Bayview's failure to timely notify Plaintiffs and California Subclass Members of the breach of their PII prevented them from taking the following remedial measures to mitigate their losses and damage from the Data Breach: (1) purchasing identity protection, monitoring, and recovery services; (2) flagging asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchasing or otherwise obtaining credit reports; (4) placing or renewing fraud alerts on a quarterly basis; (5) intensively monitoring loan data and public records; and (6) taking other steps to protect themselves and attempt to avoid or recover from identity theft.

767. As a direct and proximate result of Bayview's violations of Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiffs and California Subclass Members suffered damages, as described above and as will be proven at trial.

Lakeview

768. Lakeview is a business within the meaning of Cal. Civ. Code § 1798.80. Lakeview is a corporation organized, chartered, or holding a license or authorization certificate under the laws of Florida.

769. Lakeview owns, licenses, or maintains personal information about Californians, as required by Cal. Civ. Code § 1798.81.5(a)(1). Such PII includes, but is not limited to, the first and

¹⁶⁷ Ex. 14 (BAYVIEW000002036).

last names and Social Security numbers of Plaintiffs and California Subclass Members, along with loan numbers and other information that would permit access to Plaintiffs' and California Subclass Members' financial accounts. *See* Cal. Civ. Code §§ 1798.81.5(d)(1)(A)(i) and (iii).

770. Because Lakeview reasonably believed that Plaintiffs' and California Subclass Members' PII was acquired by unauthorized persons during the Data Breach, Lakeview had an obligation to disclose the Data Breach immediately following its discovery to the owners or licensees of the PII (*i.e.*, Plaintiffs and the California Subclass Members) as mandated by Cal. Civ. Code § 1798.82.

771. The Data Breach occurred from October 27, 2021 to December 7, 2021, and was discovered by Lakeview on December 6, 2021, but Lakeview did not disclose the Breach to Class Members until March 16, 2022.

772. By failing to disclose the Data Breach immediately following its discovery, Lakeview violated Cal. Civ. Code § 1798.82.

773. Lakeview's failure to timely notify Plaintiffs and California Subclass Members of the breach of their PII prevented them from taking the following remedial measures to mitigate their losses and damage from the Data Breach: (1) purchasing identity protection, monitoring, and recovery services; (2) flagging asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchasing or otherwise obtaining credit reports; (4) placing or renewing fraud alerts on a quarterly basis; (5) intensively monitoring loan data and public records; and (6) taking other steps to protect themselves and attempt to avoid or recover from identity theft.

774. As a direct and proximate result of Lakeview's violations of Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiffs and California Subclass Members suffered damages, as described above and as will be proven at trial.

Community Loan

775. Community Loan is a business within the meaning of Cal. Civ. Code § 1798.80. Community Loan is a corporation organized, chartered, or holding a license or authorization certificate under the laws of Delaware.

776. Community Loan owns, licenses, or maintains personal information about Californians, as required by Cal. Civ. Code § 1798.81.5(a)(1). Such PII includes, but is not limited to, the first and last names and Social Security numbers of Plaintiffs and California Subclass Members, along with loan numbers and other information that would permit access to Plaintiffs' and California Subclass Members' financial accounts. *See* Cal. Civ. Code §§ 1798.81.5(d)(1)(A)(i) and (iii).

777. Because Community Loan reasonably believed that Plaintiffs' and California Subclass Members' PII was acquired by unauthorized persons during the Data Breach, Community Loan had an obligation to disclose the Data Breach immediately following its discovery to the owners or licensees of the PII (*i.e.*, Plaintiffs and the California Subclass Members) as mandated by Cal. Civ. Code § 1798.82.

778. The Data Breach occurred from October 27, 2021 to December 7, 2021, and was discovered by Community Loan on December 6, 2021, Community Loan did not disclose the Breach to Class Members until March 16, 2022.

779. By failing to disclose the Data Breach immediately following its discovery, Community Loan violated Cal. Civ. Code § 1798.82.

780. Community Loan's failure to timely notify Plaintiffs and California Subclass Members of the breach of their PII prevented them from taking the following remedial measures to mitigate their losses and damage from the Data Breach: (1) purchasing identity protection, monitoring, and recovery services; (2) flagging asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchasing or otherwise obtaining credit reports; (4) placing or renewing fraud alerts on a quarterly basis; (5) intensively monitoring loan data and public records; and (6) taking other steps to protect themselves and attempt to avoid or recover from identity theft.

781. As a direct and proximate result of Community Loan's violations of Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiffs and California Subclass Members suffered damages, as described above and as will be proven at trial.

Pingora

782. Pingora is a business within the meaning of Cal. Civ. Code § 1798.80. Pingora is a corporation organized, chartered, or holding a license or authorization certificate under the laws of Delaware.

783. Pingora owns, licenses, or maintains personal information about Californians, as required by Cal. Civ. Code § 1798.81.5(a)(1). Such PII includes, but is not limited to, the first and last names and Social Security numbers of Plaintiffs and California Subclass Members, along with loan numbers and other information that would permit access to Plaintiffs' and California Subclass Members' financial accounts. *See* Cal. Civ. Code §§ 1798.81.5(d)(1)(A)(i) and (iii).

784. Because Pingora reasonably believed that Plaintiffs' and California Subclass Members' PII was acquired by unauthorized persons during the Data Breach, Pingora had an obligation to disclose the Data Breach immediately following its discovery to the owners or

licensees of the PII (*i.e.*, Plaintiffs and the California Subclass Members) as mandated by Cal. Civ. Code § 1798.82.

785. The Data Breach occurred from October 27, 2021 to December 7, 2021, and was discovered by Pingora on December 6, 2021, Pingora did not disclose the Breach to Class Members until March 16, 2022.

786. By failing to disclose the Data Breach immediately following its discovery, Pingora violated Cal. Civ. Code § 1798.82.

787. Pingora's failure to timely notify Plaintiffs and California Subclass Members of the breach of their PII prevented them from taking the following remedial measures to mitigate their losses and damage from the Data Breach: (1) purchasing identity protection, monitoring, and recovery services; (2) flagging asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchasing or otherwise obtaining credit reports; (4) placing or renewing fraud alerts on a quarterly basis; (5) intensively monitoring loan data and public records; and (6) taking other steps to protect themselves and attempt to avoid or recover from identity theft.

788. As a direct and proximate result of Pingora's violations of Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiffs and California Subclass Members suffered damages, as described above and as will be proven at trial.

789. Plaintiffs and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including damages, injunctive relief, and any other relief deemed appropriate by the Court.

COUNT V
UNLAWFUL AND UNFAIR CONDUCT IN VIOLATION OF
CALIFORNIA'S UNFAIR COMPETITION LAW,
Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL")
On Behalf of Plaintiffs Robert Keach, Cindy Villanueva, Pedro Rubio, Norma Grossman,
Maureen Keach, Linda Kim, and Jay Saporta and the California Subclass
Against All Defendants

790. Plaintiffs Robert Keach, Cindy Villanueva, Pedro Rubio, Norma Grossman, Maureen Keach, Linda Kim, and Jay Saporta ("Plaintiffs," for purposes of this Count) and the California Subclass, re-allege and incorporate paragraphs 1 through 625 as if fully set forth herein.

791. Plaintiffs Cindy Villanueva and Pedro Rubio bring this claim on behalf of themselves and the California Subclass against Defendants Bayview and Lakeview.

792. Plaintiffs Robert Keach, Maureen Keach, Norma Grossman, and Jay Saporta bring this claim on behalf of themselves and the California Subclass against Defendants Bayview and Pingora.

793. Plaintiff Linda Kim brings this claim on behalf of herself and the California Subclass against Defendants Bayview and Community Loan.

794. Plaintiffs lack an adequate remedy at law and assert this claim in the alternative to their other California statutory counts. There is no guarantee that Defendants will not continue the same deficient security practices that caused the Data Breach, and Defendants' continued possession of Plaintiffs' and California Subclass Members' PII presents the risk that they will be harmed again.

795. The UCL proscribes "any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." Cal. Bus. & Prof. Code § 17200.

Bayview

796. Bayview's conduct is unlawful, in violation of the UCL, because it violates the CCPA and the CCRA.

797. Bayview's conduct is substantially unfair, predatory, and contrary to California's and the nation's legislatively declared public policy in favor of protecting the privacy and security of personal and confidential information. *See* S. Rep. No. 100-500 at 7-8 (1988) (finding that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems . . . create[s] privacy interests that directly affect the ability of people to express their opinions, to join in association with others, and to enjoy the freedom and independence that the Constitution was established to safeguard."); California Bill Analysis, A.B. 375 Assem. (June 27, 2021) (noting that "[t]he unregulated and unauthorized disclosure of personal information and the resulting loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to the destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm.").

798. Bayview's unfair business acts and practices include:

- a. failing to adequately secure the personal information of Plaintiffs and California Subclass Members from disclosure to unauthorized third parties or for improper purposes;
- b. enabling the disclosure of personal and sensitive facts about Plaintiffs and California Subclass Members in a manner highly offensive to a reasonable person;

- c. enabling the disclosure of personal and sensitive facts about Plaintiffs and California Subclass Members without their informed, voluntary, affirmative, and clear consent;
- d. failing to encrypt the PII of Plaintiffs and California Subclass Members;
- e. failing to delete the PII of Plaintiffs and California subclass Members after it was no longer necessary to retain the PII;
- f. storing Plaintiffs' and California Subclass Members' PII in an internet-accessible environment when such storage was unnecessary;
- g. continuing to accept and store PII after it knew or should have known of the Data Breach;
- h. failing to monitor and detect the movement of the PII of Plaintiffs and California Subclass Members from Bayview's network to the internet in real time;
- i. failing to monitor the practices of its cybersecurity vendors;
- j. failing to include CobaltStrike—the software the attackers used—on the emergency threat feed or test its “use cases,” allowing the threat attacker to remain on Bayview's network undetected;
- k. failing to properly integrate Sentinel One—the all-important threat detection and response tool—into Bayview's Security Information and Events Management System; and
- l. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiffs and California Subclass Members from taking timely self-protection measures.

799. The gravity of harm resulting from Bayview's unfair conduct outweighs any potential utility. The failure to adequately safeguard personal, sensitive information harms the public at large and is part of a common and uniform course of wrongful conduct.

800. The harm from Bayview's conduct was not reasonably avoidable by consumers. The individuals affected by Bayview were required to provide their PII as part of their relationship with Bayview and its subsidiaries. Plaintiffs and California Subclass Members did not know of, and had no reasonable means of discovering, that their information would be exposed to hackers through inadequate data security measures. Nor did any member of the California Subclass have any means of preventing the Data Breach.

801. There were reasonably available alternatives that would have furthered Bayview's business interests of managing and storing consumer loan data, such as implementing best practices in cybersecurity defense.

802. As a direct and proximate result of Bayview's unfair methods of competition and unfair acts or practices, Plaintiffs and California Subclass Members lost money or property because their sensitive personal information experienced a diminution of value and because they paid out of pocket for credit monitoring, fraud alerts, or other identity theft protection services and devoted additional time—which they otherwise would or could have devoted to pecuniary gain—to expending additional time to monitor their credit reports and financial accounts for fraudulent activity.

Lakeview

803. Lakeview's conduct is unlawful, in violation of the UCL, because it violates the CCPA and the CCRA.

804. Lakeview’s conduct is substantially unfair, predatory, and contrary to California’s and the nation’s legislatively declared public policy in favor of protecting the privacy and security of personal and confidential information. *See* S. Rep. No. 100-500 at 7-8 (1988) (finding that “the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems . . . create[s] privacy interests that directly affect the ability of people to express their opinions, to join in association with others, and to enjoy the freedom and independence that the Constitution was established to safeguard.”); California Bill Analysis, A.B. 375 Assem. (June 27, 2021) (noting that “[t]he unregulated and unauthorized disclosure of personal information and the resulting loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to the destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm.”).

805. Lakeview’s unfair business acts and practices include:

- a. failing to adequately secure the personal information of Plaintiffs and California Subclass Members from disclosure to unauthorized third parties or for improper purposes;
- b. enabling the disclosure of personal and sensitive facts about Plaintiffs and California Subclass Members in a manner highly offensive to a reasonable person;
- c. enabling the disclosure of personal and sensitive facts about Plaintiffs and California Subclass Members without their informed, voluntary, affirmative, and clear consent;
- d. failing to require, verify, or ensure that the PII of Plaintiffs and California Subclass Members was encrypted;

- e. failing to delete the PII of Plaintiffs and California Subclass Members after it was no longer necessary to retain the PII;
- f. storing Plaintiffs' and California Subclass Members' PII in an internet-accessible environment when such storage was unnecessary;
- g. continuing to accept and store PII after it knew or should have known of the Data Breach;
- h. failing to monitor the cybersecurity practices of Bayview;
- i. failing to monitor the practices of its cybersecurity vendors; and
- j. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiffs and California Subclass Members from taking timely self-protection measures.

806. The gravity of harm resulting from Lakeview's unfair conduct outweighs any potential utility. The failure to adequately safeguard personal, sensitive information harms the public at large and is part of a common and uniform course of wrongful conduct.

807. The harm from Lakeview's conduct was not reasonably avoidable by consumers. The individuals affected by Lakeview were required to provide their PII as part of their relationship with Lakeview. Plaintiffs and California Subclass Members did not know of, and had no reasonable means of discovering, that their information would be exposed to hackers through inadequate data security measures. Nor did any member of the California Subclass have any means of preventing the Data Breach.

808. There were available alternatives that would have furthered Lakeview's business interests of managing and storing consumer loan data, such as implementing best practices in cybersecurity defense.

809. As a direct and proximate result of Lakeview’s unfair methods of competition and unfair acts or practices, Plaintiffs and California Subclass Members lost money or property because their sensitive personal information experienced a diminution of value and because they paid out of pocket for credit monitoring, fraud alerts, or other identity theft protection services and devoted additional time—which they otherwise would or could have devoted to pecuniary gain—to expending additional time to monitor their credit reports and financial accounts for fraudulent activity.

Community Loan

810. Community Loan’s conduct is unlawful, in violation of the UCL, because it violates the CCPA and the CCRA.

811. Community Loan’s conduct is substantially unfair, predatory, and contrary to California’s and the nation’s legislatively declared public policy in favor of protecting the privacy and security of personal and confidential information. *See* S. Rep. No. 100-500 at 7-8 (1988) (finding that “the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems . . . create[s] privacy interests that directly affect the ability of people to express their opinions, to join in association with others, and to enjoy the freedom and independence that the Constitution was established to safeguard.”); California Bill Analysis, A.B. 375 Assem. (June 27, 2021) (noting that “[t]he unregulated and unauthorized disclosure of personal information and the resulting loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to the destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm.”).

812. Community Loan’s unfair business acts and practices include:

- a. failing to adequately secure the personal information of Plaintiffs and California Subclass Members from disclosure to unauthorized third parties or for improper purposes;
- b. enabling the disclosure of personal and sensitive facts about Plaintiffs and California Subclass Members in a manner highly offensive to a reasonable person;
- c. enabling the disclosure of personal and sensitive facts about Plaintiffs and California Subclass Members without their informed, voluntary, affirmative, and clear consent;
- d. failing to require, verify, or ensure that the PII of Plaintiffs and California Subclass Members was encrypted;
- e. failing to delete the PII of Plaintiffs and California Subclass Members after it was no longer necessary to retain the PII;
- f. storing Plaintiffs' and California Subclass Members' PII in an internet-accessible environment when such storage was unnecessary;
- g. continuing to accept and store PII after it knew or should have known of the Data Breach;
- h. failing to monitor the cybersecurity practices of Bayview;
- i. failing to monitor the practices of its cybersecurity vendors; and
- j. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiffs and California Subclass Members from taking timely self-protection measures.

813. The gravity of harm resulting from Community Loan's unfair conduct outweighs any potential utility. The failure to adequately safeguard personal, sensitive information harms the public at large and is part of a common and uniform course of wrongful conduct.

814. The harm from Community Loan's conduct was not reasonably avoidable by consumers. The individuals affected by Community Loan were required to provide their PII as part of their relationship with Community Loan. Plaintiffs and California Subclass Members did not know of, and had no reasonable means of discovering, that their information would be exposed to hackers through inadequate data security measures. Nor did any member of the California Subclass have any means of preventing the Data Breach.

815. There were reasonably available alternatives that would have furthered Community Loan's business interests of managing and storing consumer loan data, such as implementing best practices in cybersecurity defense.

816. As a direct and proximate result of Community Loan's unfair methods of competition and unfair acts or practices, Plaintiffs and California Subclass Members lost money or property because their sensitive personal information experienced a diminution of value and because they paid out of pocket for credit monitoring, fraud alerts, or other identity theft protection services and devoted additional time—which they otherwise would or could have devoted to pecuniary gain—to expending additional time to monitor their credit reports and financial accounts for fraudulent activity.

Pingora

817. Pingora's conduct is unlawful, in violation of the UCL, because it violates the CCPA and the CCRA.

818. Pingora's conduct is substantially unfair, predatory, and contrary to California's and the nation's legislatively declared public policy in favor of protecting the privacy and security of personal and confidential information. *See* S. Rep. No. 100-500 at 7-8 (1988) (finding that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems . . . create[s] privacy interests that directly affect the ability of people to express their opinions, to join in association with others, and to enjoy the freedom and independence that the Constitution was established to safeguard."); California Bill Analysis, A.B. 375 Assem. (June 27, 2021) (noting that "[t]he unregulated and unauthorized disclosure of personal information and the resulting loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to the destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm.").

819. Pingora's unfair business acts and practices include:

- a. failing to adequately secure the personal information of Plaintiffs and California Subclass Members from disclosure to unauthorized third parties or for improper purposes;
- b. enabling the disclosure of personal and sensitive facts about Plaintiffs and California Subclass Members in a manner highly offensive to a reasonable person;
- c. enabling the disclosure of personal and sensitive facts about Plaintiffs and California Subclass Members without their informed, voluntary, affirmative, and clear consent;

- d. failing to require, verify, or ensure that the PII of Plaintiffs and California Subclass Members was encrypted;
- e. failing to delete the PII of Plaintiffs and California Subclass Members after it was no longer necessary to retain the PII;
- f. storing Plaintiffs' and California Subclass Members' PII in an internet-accessible environment when such storage was unnecessary;
- g. continuing to accept and store PII after it knew or should have known of the Data Breach;
- h. failing to monitor the cybersecurity practices of Bayview;
- i. failing to monitor the practices of its cybersecurity vendors; and
- j. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiffs and California Subclass Members from taking timely self-protection measures.

820. The gravity of harm resulting from Pingora's unfair conduct outweighs any potential utility. The failure to adequately safeguard personal, sensitive information harms the public at large and is part of a common and uniform course of wrongful conduct.

821. The harm from Pingora's conduct was not reasonably avoidable by consumers. The individuals affected by Pingora were required to provide their PII as part of their relationship with Pingora. Plaintiffs and California Subclass Members did not know of, and had no reasonable means of discovering, that their information would be exposed to hackers through inadequate data security measures. Nor did any member of the California Subclass have any means of preventing the Data Breach.

822. There were reasonably available alternatives that would have furthered Pingora's business interests of managing and storing consumer loan data, such as implementing best practices in cybersecurity defense.

823. As a direct and proximate result of Pingora's unfair methods of competition and unfair acts or practices, Plaintiffs and California Subclass Members lost money or property because their sensitive personal information experienced a diminution of value and because they paid out of pocket for credit monitoring, fraud alerts, or other identity theft protection services and devoted additional time—which they otherwise would or could have devoted to pecuniary gain—to expending additional time to monitor their credit reports and financial accounts for fraudulent activity.

824. Plaintiffs and the California Subclass accordingly seek relief under the UCL including, but not limited to, restitution to Plaintiffs and the California Subclass of money or property that the Defendants acquired by means of their unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of their unfair business practices, declaratory relief, attorneys' fees and costs, and injunctive or other equitable relief.

COUNT VI
VIOLATION OF THE FLORIDA DECEPTIVE AND
UNFAIR TRADE PRACTICES ACT,
Fla. Stat. § 501.201, *et seq.* ("FDUTPA")
On Behalf of Plaintiffs and the Class or, Alternatively, on Behalf of Plaintiffs
Wojciechowski and Scott and the Florida Subclass
Against All Defendants

825. Plaintiffs and Class Members re-allege and incorporate paragraphs 1 through 625 as if fully set forth herein.

826. Plaintiffs bring this claim on behalf of themselves and the Class against all Defendants. Alternatively, Plaintiffs Wojciechowski and Scott ("Plaintiffs," for purposes of this

Count) and the Florida Subclass re-allege and incorporate paragraphs 1 through 625 as if fully set forth herein, and bring this claim on behalf of themselves and the Florida Subclass against Defendants Bayview and Lakeview.

827. The FDUPA prohibits “unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce hereby declared unlawful.” Fla. Stat. § 501.204(1).

828. Pursuant to Fla. Stat. § 501.202, requires such claims under the FDUPA be “construed liberally” by the courts “[t]o protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce.”

829. Plaintiffs and the Class Members, as “individual[s],” are “consumer[s]” as defined by the FDUPA. *See* Fla. Stat. § 501.203(7).

Bayview

830. Bayview, on behalf of and in cooperation with its subsidiaries, obtained and stored the PII of Plaintiffs and Class Members for the purpose of allowing its subsidiaries to service loans and manage portfolios of mortgages.

831. Bayview offered, provided, or sold services in Florida and engaged in trade or commerce directly or indirectly affecting the consuming public, within the meaning of the FDUPA. *See* Fla. Stat. § 501.203.

832. Bayview’s offer, provision, and sale of services at issue in this case are “consumer transaction[s]” and Plaintiffs’ and Class Members’ PII is the subject of those “consumer transactions.” *See* Fla. Stat. § 501.212.

833. Plaintiffs and Class Members paid for or otherwise availed themselves and received services from Bayview and its affiliates, primarily for personal, family, or household purposes.

834. Bayview's acts and practices were done in the course of Bayview's and its affiliates' businesses of offering, providing, and servicing loans throughout Florida and the United States.

835. The unfair, unconscionable, and unlawful acts and practices of Bayview alleged herein, and in particular the decisions regarding data security, emanated and arose within the State of Florida, within the scope of the FDUTPA.

836. Defendant Bayview, headquartered in and operating and out of Florida, engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

- a. failing to adequately secure the personal information of Plaintiffs and Class Members from disclosure to unauthorized third parties or for improper purposes;
- b. enabling the disclosure of personal and sensitive facts about Plaintiffs and Class Members in a manner highly offensive to a reasonable person;
- c. enabling the disclosure of personal and sensitive facts about Plaintiffs and Class Members without their informed, voluntary, affirmative, and clear consent;
- d. failing to encrypt the PII of Plaintiffs and Class Members;
- e. failing to delete the PII of Plaintiffs and Class Members after it was no longer necessary to retain the PII;
- f. storing Plaintiffs' and Class Members' PII in an internet-accessible environment when such storage was unnecessary;

- g. continuing to accept and store PII after it knew or should have known of the Data Breach;
- h. failing to monitor and detect the movement of the PII of Plaintiffs and Class Members from Bayview's network to the internet in real time;
- i. failing to monitor the practices of its cybersecurity vendors;
- j. failing to include CobaltStrike—the software the attackers used—on the emergency threat feed or test its “use cases,” allowing the threat attacker to remain on Bayview's network undetected;
- k. failing to properly integrate Sentinel One—the all-important threat detection and response tool—into Bayview's Security Information and Events Management System; and
- l. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiffs and Class Members from taking timely self-protection measures.

837. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including, but not limited to, the FTC Act, 15 U.S.C. § 41, *et seq.*, and the FDUTPA, Fla. Stat. § 501.171(2).

838. Bayview knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and that the risk of a data breach or theft was high.

Lakeview

839. Lakeview serviced loans obtained by Plaintiffs and Class Members.

840. Lakeview offered, provided, or sold services in Florida and engaged in trade or commerce directly or indirectly affecting the consuming public, within the meaning of the FDUTPA. *See* Fla. Stat. § 501.203.

841. Lakeview's offer, provision, and sale of services at issue, including mortgage loan servicing, in this case are "consumer transaction[s]" and Plaintiffs' and Class Members' PII is the subject of those "consumer transactions." *See* Fla. Stat. § 501.212.

842. Plaintiffs and Class Members paid for or otherwise availed themselves and received services from Lakeview, primarily for personal, family, or household purposes.

843. Lakeview engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the procurement or provision of loan services to or for Plaintiffs and Class Members.

844. Lakeview's acts and practices were done in the course of Lakeview's business of offering, providing, and servicing loans throughout Florida and the United States.

845. The unfair, unconscionable, and unlawful acts and practices of Lakeview alleged herein, and in particular the decisions regarding data security, emanated and arose within the State of Florida, within the scope of the FDUTPA.

846. Defendant Lakeview, headquartered in and operating and out of Florida, engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

- a. failing to adequately secure the personal information of Plaintiffs and Class Members from disclosure to unauthorized third parties or for improper purposes;
- b. enabling the disclosure of personal and sensitive facts about Plaintiffs and Class Members in a manner highly offensive to a reasonable person;

- c. enabling the disclosure of personal and sensitive facts about Plaintiffs and Class Members without their informed, voluntary, affirmative, and clear consent;
- d. failing to require, verify, or ensure that the PII of Plaintiffs and Class Members was encrypted;
- e. failing to delete the PII of Plaintiffs and Class Members after it was no longer necessary to retain the PII;
- f. storing Plaintiffs' and Class Members' PII in an internet-accessible environment when such storage was unnecessary;
- g. continuing to accept and store PII after it knew or should have known of the Data Breach;
- h. failing to monitor the cybersecurity practices of Bayview;
- i. failing to monitor the practices of its cybersecurity vendors; and
- j. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiffs and Class Members from taking timely self-protection measures.

847. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including, but not limited to, the FTC Act, 15 U.S.C. § 41, *et seq.*, and the FDUTPA, Fla. Stat. § 501.171(2).

848. Lakeview knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and that the risk of a data breach or theft was high.

Pingora

849. Pingora serviced loans obtained by Plaintiffs and Class Members.

850. Pingora offered, provided, or sold services in Florida and engaged in trade or commerce directly or indirectly affecting the consuming public, within the meaning of the FDUTPA. *See* Fla. Stat. § 501.203.

851. Pingora's offer, provision, and sale of services at issue, including mortgage loan servicing, in this case are "consumer transaction[s]" and Plaintiffs' and Class Members' PII is the subject of those "consumer transactions." *See* Fla. Stat. § 501.212.

852. Plaintiffs and Class Members paid for or otherwise availed themselves and received services from Pingora, primarily for personal, family, or household purposes.

853. Pingora engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the procurement or provision of loan services to or for Plaintiffs and Class Members.

854. Pingora's acts and practices were done in the course of Pingora's business of offering, providing, and servicing loans throughout Florida and the United States.

855. The unfair, unconscionable, and unlawful acts and practices of Pingora alleged herein, and in particular the decisions regarding data security, emanated and arose within the State of Florida, within the scope of the FDUTPA.

856. Defendant Pingora, operating in and out of Florida, engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

- a. failing to adequately secure the personal information of Plaintiffs and Class Members from disclosure to unauthorized third parties or for improper purposes;

- b. enabling the disclosure of personal and sensitive facts about Plaintiffs and Class Members in a manner highly offensive to a reasonable person;
- c. enabling the disclosure of personal and sensitive facts about Plaintiffs and Class Members without their informed, voluntary, affirmative, and clear consent;
- d. failing to require, verify, or ensure that the PII of Plaintiffs and Class Members was encrypted;
- e. failing to delete the PII of Plaintiffs and Class Members after it was no longer necessary to retain the PII;
- f. storing Plaintiffs' and Class Members' PII in an internet-accessible environment when such storage was unnecessary;
- g. continuing to accept and store PII after it knew or should have known of the Data Breach;
- h. failing to monitor the cybersecurity practices of Bayview;
- i. failing to monitor the practices of its cybersecurity vendors; and
- j. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiffs and Class Members from taking timely self-protection measures.

857. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including, but not limited to, the FTC Act, 15 U.S.C. § 41, *et seq.*, and the FDUTPA, Fla. Stat. § 501.171(2).

858. Pingora knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and that the risk of a data breach or theft was high.

Community Loan

859. Community Loan serviced loans obtained by Plaintiffs and Class Members.

860. Community Loan offered, provided, or sold services in Florida and engaged in trade or commerce directly or indirectly affecting the consuming public, within the meaning of the FDUTPA. *See* Fla. Stat. § 501.203.

861. Community Loan's offer, provision, and sale of services at issue, including mortgage loan servicing, in this case are "consumer transaction[s]" and Plaintiffs' and Class Members' PII is the subject of those "consumer transactions." *See* Fla. Stat. § 501.212.

862. Plaintiffs and Class Members paid for or otherwise availed themselves and received services from Community Loan, primarily for personal, family, or household purposes.

863. Community Loan engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the procurement or provision of loan services to or for Plaintiffs and Class Members.

864. Community Loan's acts and practices were done in the course of Community Loan's business of offering, providing, and servicing loans throughout Florida and the United States.

865. The unfair, unconscionable, and unlawful acts and practices of Community Loan alleged herein, and in particular the decisions regarding data security, emanated and arose within the State of Florida, within the scope of the FDUTPA.

866. Defendant Community Loan, headquartered in and operating out of Florida, engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

- a. failing to adequately secure the personal information of Plaintiffs and Class Members from disclosure to unauthorized third parties or for improper purposes;
- b. enabling the disclosure of personal and sensitive facts about Plaintiffs and Class Members in a manner highly offensive to a reasonable person;
- c. enabling the disclosure of personal and sensitive facts about Plaintiffs and Class Members without their informed, voluntary, affirmative, and clear consent;
- d. failing to require, verify, or ensure that the PII of Plaintiffs and Class Members was encrypted;
- e. failing to delete the PII of Plaintiffs and Class Members after it was no longer necessary to retain the PII;
- f. storing Plaintiffs' and Class Members' PII in an internet-accessible environment when such storage was unnecessary;
- g. continuing to accept and store PII after it knew or should have known of the Data Breach;
- h. failing to monitor the cybersecurity practices of Bayview;
- i. failing to monitor the practices of its cybersecurity vendors; and
- j. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiffs and Class Members from taking timely self-protection measures.

867. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including, but not limited to, the FTC Act, 15 U.S.C. § 41, *et seq.*, and the FDUTPA, Fla. Stat. § 501.171(2).

868. Community Loan knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and that the risk of a data breach or theft was high.

869. Plaintiffs have standing to pursue this claim because as a direct and proximate result of Defendants' violations of the FDUTPA, Plaintiffs and Class Members have been "aggrieved" by Defendants' violations of the FDUTPA and bring this action to obtain a declaratory judgment that Defendants' acts or practices violate the FDUTPA. *See* Fla. Stat. § 501.211(1)-(2).

870. Moreover, as a direct result of Defendants' knowing violations of the FDUTPA, Plaintiffs are at a substantial present and imminent risk of identity theft. Defendants still possess Plaintiffs' and Class Members' PII, and some Plaintiffs' PII has been both accessed and misused by unauthorized third parties, which is evidence of a substantial and imminent risk of future identity theft for Plaintiffs and Class Members.

871. Plaintiffs bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit to promote the strong public interest in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs, Class Members and the public from Defendants' unfair methods of competition and unfair, unconscionable, and unlawful practices. Defendants' wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

872. The above unfair, unconscionable, and unlawful practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to

Plaintiffs and Class Members that they could not reasonably avoid and that outweighs any conceivable benefits from Defendants' violations.

873. Defendants' actions and inactions in engaging in the unfair, unconscionable, and unlawful practices described herein were negligent, knowing and willful, and/or wanton and reckless.

874. Plaintiffs and Class Members seek relief under the FDUTPA, Fla. Stat. §§ 501.201, *et seq.*, including, but not limited to, a declaratory judgment that Defendants' actions and/or practices violate the FDUTPA.

875. Plaintiffs and Class Members are also entitled to recover actual damages as set forth above, to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper. *See* Fla. Stat. § 501.211.

COUNT VII
VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS
PRACTICES ACT ("ICFA"),
815 Ill. Comp. Stat. Ann. 505, *et seq.*
On behalf of Plaintiffs Berg, Brumitt, and Cunningham and the Illinois Subclass
Against Defendants Bayview, Lakeview, and Community Loan

876. Plaintiffs Beth Berg, Albert Brumitt, and David Cunningham ("Plaintiffs," for purposes of this Count) and the Illinois Subclass re-allege and incorporate paragraphs 1 through 625 as if fully set forth herein.

877. Plaintiff Beth Berg brings this claim on behalf of herself and the Illinois Subclass against Defendants Bayview and Lakeview.

878. Plaintiffs Albert Brumitt and David Cunningham bring this claim on behalf of themselves and the Illinois Subclass against Defendants Bayview and Community Loan.

879. The ICFA prohibits “unfair methods of competition and unfair or deceptive acts or practices . . . in the conduct of any trade or commerce . . . whether any person has in fact been misled, deceived, or damaged.” 815 Ill. Comp. Stat. Ann. 505/2.

880. Plaintiffs and the Illinois Subclass Members are “person[s]” as defined by the ICFA. *See* 815 Ill. Comp. Stat. Ann. 505/1(c).

881. Plaintiffs and Illinois Subclass Members are “consumers” under the ICFA because they paid for or otherwise availed themselves of and received consumer lending services from Defendants.

882. Alternatively or additionally, Plaintiffs and Illinois Subclass Members are “consumers” in view of their relevant factual nexus to Defendants. Defendants’ challenged conduct—servicing loans and collecting borrowers’ PII without implementing adequate data security precautions—involves trade practices directed to the market generally. Plaintiffs’ and Illinois Subclass Members’ relevant actions were those of consumers in that they obtained loans and provided their PII for the purpose of servicing those loans. Defendants’ trade practices at issue concern not only Plaintiffs, but all individuals whose PII Defendants obtained. Defendants’ inadequate data security practices involve consumer protection and the concerns of consumers in that Plaintiffs and Illinois Subclass Members were required to provide their PII for their loans to be serviced by Defendants, after which Defendants’ deficient security measures compromised the confidentiality of the PII. The requested relief would benefit consumers generally by, among other things, compensating them for the damage done by Defendants’ unlawful trade practices and enjoining Defendants from continuing to maintain consumers’ PII without sufficient safeguards against its unauthorized exposure.

Bayview

883. Bayview engaged in the conduct of “trade or commerce” as defined by 815 Ill. Comp. Stat. Ann. 505/1(f). The ICFA defines “trade or commerce” as “the advertising, offering for sale, sale, or distribution of any services and any property, tangible or intangible, real, personal or mixed” *Id.* The definition “shall also include any trade or commerce directly or indirectly affecting the people of this State.” *Id.*

884. Bayview, on behalf of and in cooperation with its subsidiaries, obtained and stored the PII of Plaintiffs and Illinois Subclass Members for the purpose of allowing its subsidiaries to service loans and manage portfolios of mortgages.

885. Bayview offered, provided, or sold services in Illinois and engaged in trade or commerce directly or indirectly affecting the people of Illinois, within the meaning of the ICFA. *See* 815 Ill. Comp. Stat. Ann. 505/1(f); 815 Ill. Comp. Stat. Ann. 505/2.

886. Plaintiffs and Illinois Subclass Members paid for or otherwise availed themselves and received services from Bayview, primarily for personal, family, or household purposes.

887. Bayview’s acts and practices were done in the course of it and its affiliates’ businesses of offering, providing, and servicing loans throughout Illinois and the United States.

888. The unfair and unlawful acts and practices of Bayview alleged herein, and in particular the decisions regarding data security, emanated and arose within the State of Illinois, within the scope of the ICFA.

889. Defendant Bayview, operating in Illinois, engaged in unfair acts or practices in the conduct of trade or commerce, in violation of 815 Ill. Comp. Stat. Ann. 505/2, including but not limited to the following:

- a. failing to adequately secure the personal information of Plaintiffs and Illinois Subclass Members from disclosure to unauthorized third parties or for improper purposes;
- b. enabling the disclosure of personal and sensitive facts about Plaintiffs and Illinois Subclass Members in a manner highly offensive to a reasonable person;
- c. enabling the disclosure of personal and sensitive facts about Plaintiffs and Illinois Subclass Members without their informed, voluntary, affirmative, and clear consent;
- d. failing to encrypt the PII of Plaintiffs and Illinois Subclass Members;
- e. failing to delete the PII of Plaintiffs and Illinois Subclass Members after it was no longer necessary to retain the PII;
- f. storing Plaintiffs' and Illinois Subclass Members' PII in an internet-accessible environment when such storage was unnecessary;
- g. continuing to accept and store PII after it knew or should have known of the Data Breach;
- h. failing to monitor and detect the movement of the PII of Plaintiffs and Illinois Subclass Members from Bayview's network to the internet in real time;
- i. failing to monitor the practices of its cybersecurity vendors;
- j. failing to include CobaltStrike—the software the attackers used—on the emergency threat feed or test its “use cases,” allowing the threat attacker to remain on Bayview's network undetected;

- k. failing to properly integrate Sentinel One—the all-important threat detection and response tool—into Bayview’s Security Information and Events Management System; and
- l. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiffs and Illinois Subclass Members from taking timely self-protection measures.

890. These unfair and unlawful acts and practices violated duties imposed by laws, including, but not limited to, the FTC Act, 15 U.S.C. § 41, *et seq.*, and the ICFA, 815 Ill. Comp. Stat. Ann. 505/2.

891. Bayview knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiffs’ and Illinois Subclass Members’ PII and that the risk of a data breach or theft was high.

Lakeview

892. Lakeview engaged in the conduct of “trade or commerce” as defined by 815 Ill. Comp. Stat. Ann. 505/1(f). The ICFA defines “trade or commerce” as “the advertising, offering for sale, sale, or distribution of any services and any property, tangible or intangible, real, personal or mixed” *Id.* The definition “shall also include any trade or commerce directly or indirectly affecting the people of this State.” *Id.*

893. Lakeview serviced loans obtained by Plaintiffs and Illinois Subclass Members.

894. Lakeview offered, provided, or sold services in Illinois and engaged in trade or commerce directly or indirectly affecting the people of Illinois, within the meaning of the ICFA. *See* 815 Ill. Comp. Stat. Ann. 505/1(f); 815 Ill. Comp. Stat. Ann. 505/2.

895. Plaintiffs and Illinois Subclass Members paid for or otherwise availed themselves and received services from Lakeview, primarily for personal, family, or household purposes.

896. Lakeview engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the procurement or provision of loan services to or for Plaintiffs and Illinois Subclass Members.

897. Lakeview's acts and practices were done in the course of Lakeview's business of offering, providing, and servicing loans throughout Illinois and the United States.

898. The unfair and unlawful acts and practices of Lakeview alleged herein, and in particular the decisions regarding data security, emanated and arose within the State of Illinois, within the scope of the ICFA.

899. Defendant Lakeview, operating in Illinois, engaged in unfair acts or practices in the conduct of trade or commerce, in violation of 815 Ill. Comp. Stat. Ann. 505/2, including but not limited to the following:

- a. failing to adequately secure the personal information of Plaintiffs and Illinois Subclass Members from disclosure to unauthorized third parties or for improper purposes;
- b. enabling the disclosure of personal and sensitive facts about Plaintiffs and Illinois Subclass Members in a manner highly offensive to a reasonable person;
- c. enabling the disclosure of personal and sensitive facts about Plaintiffs and Illinois Subclass Members without their informed, voluntary, affirmative, and clear consent;
- d. failing to require, verify, or ensure that the PII of Plaintiffs and Illinois Subclass Members was encrypted;

- e. failing to delete the PII of Plaintiffs and Illinois Subclass Members after it was no longer necessary to retain the PII;
- f. storing Plaintiffs' and Illinois Subclass Members' PII in an internet-accessible environment when such storage was unnecessary;
- g. continuing to accept and store PII after it knew or should have known of the Data Breach;
- h. failing to monitor the cybersecurity practices of Bayview;
- i. failing to monitor the practices of its cybersecurity vendors; and
- j. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiffs and Illinois Subclass Members from taking timely self-protection measures.

900. These unfair and unlawful acts and practices violated duties imposed by laws, including, but not limited to, the FTC Act, 15 U.S.C. § 41, *et seq.*, and the ICFA, 815 Ill. Comp. Stat. Ann. 505/2.

901. Lakeview knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiffs' and Illinois Subclass Members' PII and that the risk of a data breach or theft was high.

Community Loan

902. Community Loan engaged in the conduct of "trade or commerce" as defined by 815 Ill. Comp. Stat. Ann. 505/1(f). The ICFA defines "trade or commerce" as "the advertising, offering for sale, sale, or distribution of any services and any property, tangible or intangible, real, personal or mixed" *Id.* The definition "shall also include any trade or commerce directly or indirectly affecting the people of this State." *Id.*

903. Community Loan serviced loans obtained by Plaintiffs and Illinois Subclass Members.

904. Community Loan offered, provided, or sold services in Illinois and engaged in trade or commerce directly or indirectly affecting the people of Illinois, within the meaning of the ICFA. *See* 815 Ill. Comp. Stat. Ann. 505/1(f); 815 Ill. Comp. Stat. Ann. 505/2.

905. Plaintiffs and Illinois Subclass Members paid for or otherwise availed themselves and received services from Community Loan, primarily for personal, family, or household purposes.

906. Community Loan engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the procurement or provision of loan services to or for Plaintiffs and Illinois Subclass Members.

907. Community Loan's acts and practices were done in the course of Community Loan's business of offering, providing, and servicing loans throughout Illinois and the United States.

908. The unfair and unlawful acts and practices of Community Loan alleged herein, and in particular the decisions regarding data security, emanated and arose within the State of Illinois, within the scope of the ICFA.

909. Defendant Community Loan, operating in Illinois, engaged in unfair acts or practices in the conduct of trade or commerce, in violation of 815 Ill. Comp. Stat. Ann. 505/2, including but not limited to the following:

- a. failing to adequately secure the personal information of Plaintiffs and Illinois Subclass Members from disclosure to unauthorized third parties or for improper purposes;

- b. enabling the disclosure of personal and sensitive facts about Plaintiffs and Illinois Subclass Members in a manner highly offensive to a reasonable person;
- c. enabling the disclosure of personal and sensitive facts about Plaintiffs and Illinois Subclass Members without their informed, voluntary, affirmative, and clear consent;
- d. failing to require, verify, or ensure that the PII of Plaintiffs and Illinois Subclass Members was encrypted;
- e. failing to delete the PII of Plaintiffs and Illinois Subclass Members after it was no longer necessary to retain the PII;
- f. storing Plaintiffs' and Illinois Subclass Members' PII in an internet-accessible environment when such storage was unnecessary;
- g. continuing to accept and store PII after it knew or should have known of the Data Breach;
- h. failing to monitor the cybersecurity practices of Bayview;
- i. failing to monitor the practices of its cybersecurity vendors; and
- j. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiffs and Illinois Subclass Members from taking timely self-protection measures.

910. These unfair and unlawful acts and practices violated duties imposed by laws, including, but not limited to, the FTC Act, 15 U.S.C. § 41, *et seq.*, and the ICFA, 815 Ill. Comp. Stat. Ann. 505/2.

911. Community Loan knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiffs' and Illinois Subclass Members' PII and that the risk of a data breach or theft was high.

912. Plaintiffs have standing to pursue this claim because as a direct and proximate result of Bayview's, Lakeview's, and Community Loan's violations of the ICFA, Plaintiffs and Illinois Subclass Members have suffered pecuniary losses, among other actual damages. *See* 815 Ill. Comp. Stat. Ann. 505/10a.

913. Plaintiffs also have standing to pursue this claim because, as a direct result of Bayview's, Lakeview's, and Community Loan's knowing violations of the ICFA, Plaintiffs are at a substantial present and imminent risk of identity theft. Bayview, Lakeview, and/or Community Loan still possess Plaintiffs' and Illinois Subclass Members' PII, and some of Plaintiffs' PII has been both accessed and misused by unauthorized third parties, which is evidence of a substantial and imminent risk of future identity theft for Plaintiffs and all Illinois Subclass Members.

914. The above unfair and unlawful practices and acts by Bayview, Lakeview, and Community Loan were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

915. Bayview's, Lakeview's, and Community Loan's actions and inactions in engaging in the unfair and unlawful practices described herein were negligent, knowing, and willful, and/or wanton and reckless.

916. Plaintiffs and Illinois Subclass Members therefore seek relief under the ICFA, 815 Ill. Comp. Stat. Ann. 505, *et seq.*, including, but not limited to, actual damages as set forth above and a declaratory judgment that Defendants' actions and/or practices violate the ICFA.

917. Plaintiffs and Illinois Subclass Members are also entitled to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper. *See* 815 Ill. Comp. Stat. Ann. 505/10a.

COUNT VIII
VIOLATIONS OF THE NEW YORK GENERAL BUSINESS LAW ("GBL"),
N.Y. Gen. Bus. Law § 349, *et seq.*
On Behalf of Plaintiff Hardik Sevak and the New York Subclass
Against Defendant Lakeview

918. Plaintiff Hardik Sevak ("Plaintiff" for purposes of this count) and the New York Subclass re-allege and incorporate paragraphs 1 through 625 as if fully set forth herein.

919. Plaintiff Hardik Sevak brings this claim on behalf of himself and the New York Subclass against Defendant Lakeview.

920. The GBL prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce" N.Y. Gen. Bus. Law § 349.

921. Lakeview serviced loans obtained by Plaintiff and New York Subclass Members.

922. Plaintiff and New York Subclass Members paid for or otherwise availed themselves and received services from Lakeview, primarily for personal, family, or household purposes.

923. Lakeview engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the procurement or provision of loan services to or for Plaintiff and New York Subclass Members.

924. Lakeview's acts and practices were done in the course of Lakeview's business of offering, providing, and servicing loans throughout New York and the United States.

925. Lakeview engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

- a. failing to adequately secure the personal information of Plaintiff and New York Subclass Members from disclosure to unauthorized third parties or for improper purposes;
- b. enabling the disclosure of personal and sensitive facts about Plaintiff and New York Subclass Members in a manner highly offensive to a reasonable person;
- c. enabling the disclosure of personal and sensitive facts about Plaintiff and New York Subclass Members without their informed, voluntary, affirmative, and clear consent;
- d. failing to require, verify, or ensure that the PII of Plaintiff and New York Subclass Members was encrypted;
- e. failing to delete the PII of Plaintiff and New York Subclass Members after it was no longer necessary to retain the PII;
- f. storing Plaintiff's and New York Subclass Members' PII in an internet-accessible environment when such storage was unnecessary;
- g. continuing to accept and store PII after it knew or should have known of the Data Breach;
- h. failing to monitor the cybersecurity practices of Bayview;
- i. failing to monitor the practices of its cybersecurity vendors;
- j. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiff and New York Subclass Members from taking timely self-protection measures;

- k. misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and New York Subclass Members' PII, including by implementing and maintaining reasonable security measures;
- l. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and New York Subclass Members' PII; and
- m. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass Members' PII, including duties imposed by the FTC Act, and N.Y. Gen. Bus. Law § 899-aa.

926. Lakeview's material misrepresentations include its statements in its Privacy Policy provided to borrowers that Lakeview would "maintain commercially reasonable security measures" to protect Plaintiff's and New York Subclass Members' PII from "unauthorized access," when it failed to do so, and that Lakeview would "use industry-standard encryption to protect data" when, in fact, it was storing unencrypted PII, including unencrypted Social Security numbers. Lakeview's representations and omissions regarding its data security were material because they were likely to deceive reasonable consumers about the adequacy of Lakeview's data security and ability to safeguard its consumers' confidential PII—matters of importance to a reasonable consumer transacting under the circumstances.

927. Lakeview's representations and omissions caused injury to Plaintiff. Had Plaintiff known that Lakeview's data security was inadequate to prevent the unauthorized disclosure of his PII, Plaintiff would not have provided his PII to Lakeview. Reasonable and ordinary means,

including written communications via U.S. mail, of notifying Plaintiff of its inadequate data security were available to Lakeview.

928. As a direct and proximate result of Lakeview's deceptive and unlawful acts and practices, Plaintiff and New York Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

929. Lakeview's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large.

930. The above deceptive and unlawful practices and acts by Lakeview caused substantial injury to Plaintiff and New York Subclass Members that they could not reasonably avoid.

931. Plaintiff and New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages as set forth above or statutory damages of \$50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

COUNT IX
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT ("CPA")
RCW 19.86.010, et seq.,
On Behalf of Plaintiff Mark Arthur and the Washington Subclass
Against Defendants Bayview and Pingora

932. Plaintiff Mark Arthur ("Plaintiff" for purposes of this count) and the Washington Subclass Members re-allege and incorporate paragraphs 1 through 625 as if fully set forth herein.

933. Plaintiff brings this claim on behalf of himself and the Washington Subclass Members against Defendants Bayview and Pingora.

934. The Washington State Consumer Protection Act, RCW 19.86.020 (the “CPA”) prohibits any “unfair or deceptive acts or practices” in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

Bayview

935. Bayview is a “person” as described in RWC 19.86.010(1).

936. Bayview engages in “trade” and “commerce” as described in RWC 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

937. Bayview, on behalf of and in cooperation with its subsidiaries, obtained and stored the PII of Plaintiff and Washington Subclass Members for the purpose of allowing its subsidiaries to service loans and manage portfolios of mortgages.

938. Plaintiff and Washington Subclass Members paid for or otherwise availed themselves and received services from Bayview, primarily for personal, family, or household purposes.

939. Bayview’s acts and practices were done in the course of it and its affiliates’ businesses of offering, providing, and servicing loans throughout Washington and the United States.

940. Bayview engaged in unlawful and unfair practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of the CPA, including:

- a. failing to adequately secure the personal information of Plaintiff and Washington Subclass Members from disclosure to unauthorized third parties or for improper purposes;

- b. enabling the disclosure of personal and sensitive facts about Plaintiff and Washington Subclass Members in a manner highly offensive to a reasonable person;
- c. enabling the disclosure of personal and sensitive facts about Plaintiff and Washington Subclass Members without their informed, voluntary, affirmative, and clear consent;
- d. failing to encrypt the PII of Plaintiff and Washington Subclass Members;
- e. failing to delete the PII of Plaintiff and Washington Subclass Members after it was no longer necessary to retain the PII;
- f. storing Plaintiff's and Washington Subclass Members' PII in an internet-accessible environment when such storage was unnecessary;
- g. continuing to accept and store PII after it knew or should have known of the Data Breach;
- h. failing to monitor and detect the movement of the PII of Plaintiff and Washington Subclass Members from Bayview's network to the internet in real time;
- i. failing to monitor the practices of its cybersecurity vendors;
- j. failing to include CobaltStrike—the software the attackers used—on the emergency threat feed or test its “uses cases,” allowing the threat attacker to remain on Bayview's network undetected;
- k. failing to properly integrate Sentinel One—the all-important threat detection and response tool—into Bayview's Security Information and Events Management System; and

1. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiff and Washington Subclass Members from taking timely self-protection measures.

941. By reason of the above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Bayview engaged in unlawful and unfair practices within the meaning, and in violation, of the CPA.

942. Bayview's above-described wrongful actions, inaction, omissions, and want of ordinary care also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Bayview's wrongful conduct is substantially injurious to numerous citizens and was and is able capable of causing such harm.

943. Likewise, Bayview's acts, practices, and omissions harm the public interest because they injured numerous citizens and were and are able capable of causing such harm.

944. The gravity of Bayview's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Bayview's legitimate business interests other than engaging in the above-described wrongful conduct.

Pingora

945. Pingora is a "person" as described in RWC 19.86.010(1).

946. Pingora engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

947. Plaintiff and Washington Subclass Members paid for or otherwise availed themselves and received services from Pingora, primarily for personal, family, or household purposes.

948. Pingora engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the procurement or provision of loan services to or for Plaintiff and Washington Subclass Members.

949. Pingora's acts and practices were done in the course of Pingora's business of offering, providing, and servicing loans throughout Washington and the United States.

950. Pingora engaged in unlawful and unfair practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of the CPA, including:

- a. failing to adequately secure the personal information of Plaintiff and Washington Subclass Members from disclosure to unauthorized third parties or for improper purposes;
- b. enabling the disclosure of personal and sensitive facts about Plaintiff and Washington Subclass Members in a manner highly offensive to a reasonable person;
- c. enabling the disclosure of personal and sensitive facts about Plaintiff and Washington Subclass Members without their informed, voluntary, affirmative, and clear consent;
- d. failing to require, verify, or ensure that the PII of Plaintiff and Washington Subclass Members was encrypted;
- e. failing to delete the PII of Plaintiff and Washington Subclass Members after it was no longer necessary to retain the PII;
- f. storing Plaintiff's and Washington Subclass Members' PII in an internet-accessible environment when such storage was unnecessary;

- g. continuing to accept and store PII after it knew or should have known of the Data Breach;
- h. failing to monitor the cybersecurity practices of Bayview;
- i. failing to monitor the practices of its cybersecurity vendors; and
- j. unreasonably delaying in providing notice of the Data Breach and thereby preventing Plaintiff and Washington Subclass Members from taking timely self-protection measures.

951. By reason of the above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Pingora engaged in unlawful and unfair practices within the meaning, and in violation, of the CPA.

952. Pingora's above-described wrongful actions, inaction, omissions, and want of ordinary care also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Pingora's wrongful conduct is substantially injurious to numerous citizens and was and is able capable of causing such harm.

953. Likewise, Pingora's acts, practices, and omissions harm the public interest because they injured numerous citizens and were and are able capable of causing such harm.

954. The gravity of Pingora's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Pingora's legitimate business interests other than engaging in the above-described wrongful conduct.

955. Plaintiff and the Washington Subclass seek all monetary and non-monetary relief allowed by law, including actual damages as set forth above, treble damages, injunctive relief, and attorney's fees and costs.

COUNT X
DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
On Behalf of All Plaintiffs and the Class
Against All Defendants

956. Plaintiffs re-allege and incorporate paragraphs 1 through 625 as if fully set forth herein.

957. Plaintiffs bring this count on behalf of themselves and the Class. This count is brought against all Defendants.

958. The Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, authorizes this Court to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

959. Defendants owe duties of care to Plaintiffs and Class Members which require them to adequately secure their PII.

960. Defendants still possess Plaintiffs' and Class members' PII.

961. Defendants do not specify in their Data Breach notification letters what steps they have taken to prevent a similar breach from occurring again.

962. Plaintiffs and Class Members are at risk of harm due to the exposure of their PII and Defendants' failures to address the security failings that lead to such exposure.

963. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' PII and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and the Class from further data breaches that compromise their PII.

964. Plaintiffs and the Class, therefore, seek a declaration that (1) each of Defendants' existing security measures do not comply with their obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect consumers' Personal Information, and (2) to comply with their duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

- a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;
- b. Engaging third-party security auditors and internal personnel to run automated security monitoring;
- c. Auditing, testing, and training their security personnel regarding any new or modified procedures;
- d. Segmenting user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;
- e. Conducting regular database scanning and security checks;
- f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- g. Purchasing credit monitoring services for Plaintiffs and Class Members for their respective lifetimes; and

- h. Meaningfully educating Plaintiffs and Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

965. The Court should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with the law and industry standards to protect Plaintiffs' and Class Members' PII.

966. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Defendants' systems or networks. The risk of another breach is real, immediate, and substantial.

967. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. If another data breach occurs, Plaintiffs and the Class will likely be subjected to fraud, identity theft, and other harms described herein. But, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is minimal given they have preexisting legal obligations to employ these measures.

PRAYER FOR RELIEF

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

- A. An Order certifying the Class and the Subclasses, as defined herein, and appointing Plaintiffs and their counsel to represent the Class and Subclasses;
- B. Equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete, and accurate

disclosures to Plaintiffs and Class Members;

- C. Injunctive relief requested by Plaintiffs, 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 their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendants to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes;
 - iv. requiring Defendants to delete, destroy, and purge the PII 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;
 - v. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;
 - vi. prohibiting Defendants from maintaining Plaintiffs' and Class Members' personally identifying information on a cloud-based database;
 - vii. 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;
- viii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;
 - ix. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;
 - x. 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;
 - xi. requiring Defendants to conduct regular database scanning and securing checks;
 - xii. 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;
 - xiii. 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;

- xiv. requiring Defendants to implement a system of tests to assess their 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;
 - xv. 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;
 - xvi. requiring Defendants to adequately educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;
 - xvii. 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: March 28, 2024

Respectfully submitted,

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

Liaison Counsel

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

*Chair, Plaintiffs' Executive
Committee*

ADAM E. POLK (*pro hac vice*)
JORDAN ELIAS (*pro hac vice*)
SIMON GRILLE (*pro hac vice*)
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, CA 94108
Telephone: (415) 981-4800

apolk@girardsharp.com
jelias@girardsharp.com
sgrille@girardsharp.com

STUART ANDREW DAVIDSON
NICOLLE B. BRITO
**ROBBINS GELLER RUDMAN &
DOWD LLP**

225 N.E. Mizner Boulevard, Suite
720

Boca Raton, FL 33432

561-750-3000

Fax: 750-3364

sdavidson@rgrdlaw.com

nbrito@rgrdlaw.com

RACHELE R. BYRD (*pro hac vice*)

**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

*Members, Plaintiffs' Executive
Committee*

TERRY R. COATES (*pro hac vice*)

DYLAN J. GOULD (*pro hac vice*

forthcoming)

**MARKOVITS, STOCK &
DEMARCO, LLC**

119 E. Court Street, Suite 530

Cincinnati, OH 45202

Telephone: 513/651-3700

513/665-0219 (fax)

tcoates@msdlegal.com

dgould@msdlegal.com

M. ANDERSON BERRY (*pro hac vice*)

GREGORY HAROUTUNIAN (*pro hac vice* forthcoming)

**CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.**

865 Howe Avenue

Sacramento, CA 95825

Telephone: (916) 239-4778

Facsimile: (916) 924-1829

aberry@justice4you.com

gharoutunian@justice4you.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

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

LORI G. FELDMAN (*pro hac vice*)

GEORGE GESTEN

MCDONALD, PLLC

102 Half Moon Bay Drive

Croton-on-Hudson, New York 10520

Phone: (917) 983-9321

Fax: (888) 421-4173

Email: LFeldman@4-Justice.com

E-Service: eService@4-Justice.com

Additional Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

The undersigned certifies that, on March 28, 2024, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF. I also certify the foregoing document is being served today on all counsel of record in this case via transmission of Notice of Electronic Filing generated by CM/ECF.

/s/ Julie Braman Kane
JULIE BRAMAN KANE

Exhibit “1”

LAKEVIEW LOAN SERVICING, LLC

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

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 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.

What You Can Do.

We engaged Kroll, a third party with monitoring expertise, to provide identity monitoring services at no cost to you for one year. The identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information on your complimentary one-year membership, as well as additional steps you can take in response to the incident, please see the additional information provided in this letter and visit info.krollmonitoring.com.

For More Information

If you have questions about this notice, please call (855) 541-3564 from 8:00 a.m. – 5:30 p.m. Central Time, Monday through Friday (excluding major US holidays).

Sincerely,



Judith Tribble
SVP, Chief Compliance Officer
Lakeview Loan Servicing, LLC



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

PINGORA LOAN SERVICING, LLC

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Pingora Loan Servicing, LLC ("Pingora") 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?

Pingora currently or previously owned the servicing rights to a mortgage loan you have or had and used a third party to provide servicing of your loan. A security incident involving unauthorized access to Pingora file servers was identified in early December 2021. Steps were immediately taken to contain the incident, notify law enforcement, and a forensic 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 March 7, 2022, the review process generated a list of individuals, including you, whose name, address, loan number, and Social Security number were included in the files. 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.

What You Can Do.

We engaged Kroll, a third party with monitoring expertise, to provide identity monitoring services at no cost to you for one year. The identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information on your complimentary one-year membership, as well as additional steps you can take in response to the incident, please see the additional information provided in this letter and visit info.krollmonitoring.com.

For More Information.

If you have questions about this notice, please call 1-855-541-3607 from 8:00 a.m. – 5:30 p.m. Central Time, Monday through Friday (excluding major US holidays).

Sincerely,



Ron Bendalin, Chief Compliance Officer
Pingora Loan Servicing, LLC



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Exhibit “2”



Online Privacy Notice

Lakeview Loan Servicing, LLC (“Lakeview” or “Company”) recognizes the importance of keeping the personal information you provide to us private and secure. Lakeview has developed a comprehensive privacy policy and we use the latest technology to ensure that your personal information is secure. Lakeview respects your privacy and is committed to providing a transparent notice of our Privacy Notice and Disclosure for California Residents. This Privacy Notice and Disclosure for California Residents applies solely to those who reside in the State of California (“consumers” or “you”). The purpose of this privacy notice and disclosure is to inform California residents, at or before the time of collection of personal information and to inform you as part of our privacy policies.

Lakeview reserves the right to change this policy at any time.

Information We May Collect

Lakeview may collect certain types of information from you, such as information you voluntarily provide via forms, surveys, applications, etc. when you visit the Company’s sites. We may also collect information about you from your online browsing and transactions, including your preferences, pages visited, technical information regarding your computer and operating systems, such as your Internet Protocol (IP) address, domain name and system configuration and settings.

Links

At certain places on this site, live “links” to other Internet addresses can be accessed (“Linked Sites”). Such Linked Sites contain information created, published, maintained, or otherwise posted by institutions or organizations independent of Lakeview does not endorse, approve, certify or control these



Linked Sites and does not guarantee the accuracy, completeness, efficacy, timeliness or correct sequencing of information that they contain. Lakeview's Privacy Policy does not apply to these Linked Sites. The privacy policies of these Linked Sites may differ from Lakeview's, and you should review their policies before accessing them and/or submitting information. Lakeview is not responsible for the privacy or security of these sites, including the accuracy, completeness, reliability or suitability of their information. If you are asked to provide information on one of these websites, you are strongly urged to carefully study their privacy policies before sharing your information.

Cookies

Cookies are pieces of information stored directly on the computer you are using. The Company, or any of the Company's third-party advertising service providers, may place cookies or similar files on your hard drive for security purposes, to facilitate site navigation and to personalize your experience while visiting the Company's sites. Cookies allow the Company's to collect technical and navigational information, such as browser type, time spent on its respective site and pages visited. Cookies allow the Company to select which of its advertisements or offers are most likely to appeal to you and display them while you are on the Company's websites. The Company may also use cookies in online advertising to track consumer responses to the Company's advertisements and may use cookies or other files to track your use of other websites. Cookies and other technologies provide the Company the capability to monitor the use of the Company's websites so the Companies can continually improve the design and functionality to better serve you. Cookies and similar files do not contain or capture unencrypted personally identifiable data.

If you do not accept these cookies, you may experience some inconvenience in your use of some online options. You also may not receive advertising or other offers from the Company that are relevant to your interests and needs. The Company uses web-browsing cookies to display information more effectively to you and to gather data about the usage of the Company's websites.

At times, Lakeview may use other technologies to capture customer specific data to help understand how customers use its sites and to assist us with resolving



customers' questions regarding the use of our online sites.

Advertising

Lakeview advertises on pages within its websites as well as on other websites not affiliated with the Company. The Company may contract with another organization to advertise to you through the use of cookies, social media platforms and web beacons.

Information collected through cookies, social media platforms and web beacons includes the number of people who look at each of the pages on the Company's websites, social media platforms, search engine referrals, browsing patterns within the Company's websites, and responses to advertisements and promotions on social media platform or the Company's websites. Information collected may also include other trends and activity on the Company's websites, social media platforms, and basic information about whether you have visited the sites before, your Internet connection and computer settings, such as your browser, your IP address and your time zone.

From time to time, consumers will experience 'Pop Ups' from other companies while visiting the Company's sites. Pop Ups are generated by 'Adware' placed on your computer when other sites have been visited. Lakeview does not participate in the use of Adware.

Advertising on the Company's Websites

The Companies advertise their respective products and services, on pages within the Company's websites. These advertisements may take the form of banner ad, and other applicable formats.

Advertising on other Websites or Social Media platforms

Lakeview contracts advertising with other companies to advertise the Company's information and services on websites not affiliated with Lakeview. If you click on one of the Lakeview ads, you link to the particular Company website that offers the advertised service. These ads may contain cookies that allow tracking of your response to the Company's advertisements. These cookies do not identify you



personally. Lakeview prohibits any company that places Lakeview ads from using this information for any purpose other than to assist us in measuring the effectiveness of the Lakeview ads.

How the Companies use and share information

Unless otherwise described in this policy, Lakeview will use and share any information that the Company collect from or about you that is covered by this policy in accordance with this Privacy Policy.

The Company may also share aggregated or anonymous data about the Company's customers and visitors to the Company's websites with advertising service providers and with companies that help Lakeview understand how you use its websites.

Looking out for children

Lakeview does not knowingly market to or solicit information from children under 13 without parental consent. Lakeview recognizes that protecting children's identities and privacy online is important, and that the responsibility to do so rests with both the online industry and with parents. While the Company works to protect your personal information, you also have responsibility.

Internet safety for children. The Internet is a public network. Children's access to the Internet can allow them to visit inappropriate websites and be exposed to unwanted risks. COPPA, the Children's Online Privacy Protection Act, protects children under the age of 13 from the online collection of personal information. Learn more about COPPA on the [Federal Trade Commission's website](#). Parents can be proactive by installing filtering software that gives them more control over their family's Internet experience.

Lakeview recommends that minors 13 years of age or older ask their parents for permission before sending any information about themselves to anyone over the Internet.

Security



We maintain commercially reasonable security measures to protect the personal information we collect and store from loss, misuse, destruction, or unauthorized access. Our security includes physical, administrative, and technology-based measures. We use industry-standard encryption to protect data in transit and at rest. Our internal policies and procedures impose a number of standards to safeguard the confidentiality of personal information, prohibit the unlawful disclosure of personal information, and limit access to personal information. While we undertake these security measures, you acknowledge that no security measure or modality of data transmission over the Internet can be guaranteed to be 100% secure. We take security seriously; however, you should not expect that any personal information provided to us through the Site is free from the risk posed by unauthorized access.

Your Internet session is encrypted if your security-enabled browser is connected to a web site using the Secure Hypertext Transport Protocol. URL strings beginning with “HTTPS://” instead of the usual “HTTP://” indicate that the secure protocol is in effect. Your browser may also tell you if security is operating. For example, Netscape Navigator may display the icon in the lower left corner of your screen in secure mode. If 128-bit security is in effect, it shows the icon. Microsoft Internet Explorer shows an icon in either case. Note that security may be operating without any visible indication if the web page you are viewing employs frames (see below). If secure transmission is not in effect or only part of a frame-based page is secure, Netscape shows the “broken key” icon, and Explorer does not show the “lock” icon.

CALIFORNIA PRIVACY RIGHTS NOTICE

Additional Notice for California Residents

At Lakeview, we are mindful of our responsibilities under the California Consumer Protection Act (“CCPA”) (Cal. Civ. Code § 1798.100 et seq.) regarding the collection, use, and disclosure of your personal information, both online and offline. This online notice applies only to California residents who are subject to the CCPA.

Most visitors of our website are either representatives of businesses seeking to interact with us as part of their jobs, or individuals engaging with us in connection with using our financial products or services. Please note that personal information we obtain, use, or is disclosed through these business-to-business interactions or



pursuant to the Gramm-Leach-Bliley Act (“GLBA”), or the California Financial Information Privacy Act (“CFIPA”) are exempt from the CCPA.

How We Collect, Use, and Share Personal Information

1. Personal Information of California Residents Collected in the Last Twelve Months

We collect information that identifies, relates to, describes, references, and is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household (“Personal Information”). In particular, we have obtained the following categories of Personal Information on California residents within the last twelve months:

Identifiers such as real name, alias, postal address, email address, IP address, unique personal identifier, online identifier, account name, social security number, and driver’s license number, passport number or other government issued number, when you submit this information to create an account, apply for a loan, request to learn more about our financial products and services, or subscribe to email alerts.

Any information that identifies, relates to, describes, or is capable of being associated with a particular consumer or household, including, the “identifiers” listed in (A), and the following: signature, insurance policy number, employment, employment history, bank account number, credit card number, debit card number, or any other financial information when you apply for or receive a loan which was then provided to us when we became your master servicer.

The following categories of protected classification characteristics under California or federal law: date of birth/age (40 years or older), gender, race, color, national origin, citizenship, or marital status, when you provide it to us.

Internet or other similar network activity information, including, but not limited to, browsing history on our websites, search history, and information on your interaction with our websites or applications when you choose to visit and interact with our websites or applications.

Audio information such as recordings of when you called into our customer contact line; visual images from security cameras in our branch offices; and electronic



information in the form of Internet or other electronic network activity information, as described above.

Current or past professional or employment-related information, including job history, performance evaluations, position details, or references.

For each of the above categories, most of the Personal Information we have obtained was provided by you as part of your mortgage origination process, which was then provided to us when we became your mortgage servicer, or information we received from third parties in connection with processing, underwriting, funding, and servicing your loan. This information is necessary for us to complete your mortgage loan transaction or transact as a mortgage servicer in accordance with federal and state law.

We use commercially reasonable security measures to protect the information we have obtained, in accordance with federal and state regulations. Please visit our Privacy Policy for more information about the security measures to maintain information.

Please note that Personal Information does not include:

- Publicly available information from government records
- De-identified or aggregated consumer information; and
- Information exempted from the CCPA's scope, including without limitation, the GLBA, the Fair Credit Reporting Act (FCRA), California Financial Information Privacy Act (CFIPA), the Driver's Privacy Protection Act of 1994, and certain information associated with business-to-business transactions.

2. Our Use of Personal Information for Business Purposes in the Last Twelve Months

We use the Personal Information we obtain, identified in each of the above categories, for the business purposes listed below.

- Audits and reporting relating to particular transactions and interactions, including online interactions, you may have with us or others on our behalf



- Detecting and protecting against security incidents, and malicious, deceptive, fraudulent or illegal activity, and prosecuting the same
- Debugging to identify and repair errors in our systems;
- Providing services on our behalf or on behalf of another, including maintaining or servicing accounts, providing customer service, fulfilling transactions, verifying identity information, processing payments, and other services;
- Conducting internal research to develop and demonstrate technology;
- Conducting activity to verify, enhance, and maintain the quality or safety of services or devices which we may own, control, or provide;
- Preparing statistics and performing analysis to support our operations;
- Conducting surveys regarding our products, services, and client satisfaction; and
- Receiving and responding to inquiries.

3. Our Sharing of Personal Information in the Last Twelve Months

Disclosures of Personal Information for Business Purposes

Lakeview does not share any information about you or your company to unaffiliated third parties, except as necessary to process, underwrite, fund and service your loan and as permitted by law. Within the last twelve months, we have disclosed Personal Information identified in the Categories A-F above only (i) at your express request; (ii) as part of an exempt business-to-business commercial transaction; (iii) in connection with providing you a financial service or product for personal, family, or household, pursuant to the GLBA; or (iv) to our service providers for the business purpose(s) described above.

When we disclose Personal Information for a business purpose, we execute a contract that describes the purpose and requires the recipient to keep Personal Information confidential and not use it for any purpose except performing the contract.

No Sales of Personal Information



We do not sell Personal Information within the meaning of the CCPA nor do we plan to sell Personal Information. If that changes, we will let you know in advance and provide you with information so that you may understand and exercise your right to opt-out of the future sale of your Personal Information.

Please note that we do not collect, use, sell or disclose Personal Information of individuals we know to be under the age of 18 to business partners or third parties.

Privacy Rights and Choices for California Residents

If you are a California resident, the CCPA provides you with certain rights related to your Personal Information. This section describes your CCPA rights and explains how to exercise those rights.

As discussed above, the CCPA does not apply to all or nearly all information we obtain, use, or share as part of our role as a financial institution or resulting from certain business-to-business transactions. We will, however, continue to evaluate our business-to-business activities throughout 2021 and update our Privacy Policy consistent with California laws and regulations, where applicable.

Access to Personal Information and Data Portability

You have the right to know what Personal Information we have obtained and disclosed about you for a business purpose in the last twelve months. Once we receive and confirm your verifiable consumer request, we will disclose to you any or all of the following:

- The categories of Personal Information we collected about you;
- The categories of sources from which the Personal Information was collected;
- Our business or commercial purpose for collecting that Personal Information;
- The categories of third parties with whom we share that Personal Information;
- The specific pieces of Personal Information we collected about you (or portability request); and
- If we disclosed your Personal Information for a business purpose, a disclosure identifying the categories of Personal Information that each category of recipient obtained.



- We are not required to comply with a verifiable consumer request for access or data portability twice within a 12-month period.

Deletion Request

You have the right to request that we delete (and direct our service providers to delete) Personal Information we collected about you and retained, subject to certain exceptions.

We may deny your deletion request if retaining the information is necessary for us or our service provider(s) to:

- complete the transaction for which we collected the Personal Information,
- provide a good or service that you requested,
- take actions reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform our contract with you;
- detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for such activities;
- debug products to identify and repair errors that impair existing intended functionality;
- exercise free speech, ensure the right of another consumer to exercise their free speech rights, or exercise another right provided for by law;
- comply with the California Electronic Communications Privacy Act;
- engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the information's deletion may likely render impossible or seriously impair the research's achievement,
- if you previously provided informed consent;
- enable solely internal uses that are reasonably aligned with consumer expectations based on your relationship with us;
- comply with a legal obligation; or
- make other internal and lawful uses of that information that are compatible with the context in which you provided it.



Opt-out of Sale of Personal Information

The CCPA provides you with the right to direct us to not sell your Personal Information. However, as discussed above, we do not engage in the sale of Personal Information as contemplated by the CCPA.

Non-Discrimination

We will not discriminate against you for exercising any of your CCPA rights. This means that we may not deny you goods or services, charge you different prices or rates for services or provide you with a different level or quality of services (or suggest that we will do so), in response to a request made under the CCPA.

We may, however, charge different prices or rates, or provide a different level or quality of goods or services, if that difference is reasonably related to the value provided to us by your Personal Information.

Exercising Your CCPA Rights

To exercise one or more of the above rights, you or someone you authorize, may submit a request by:

Writing us at Lakeview. Compliance Department, 4425 Ponce De Leon Boulevard, 5th Floor, Coral Gables, FL 33146 or email at privacy@lakeview.com. Reminder: please include the statement “Attention: California Privacy Rights Request” in the subject line of your email or within the body of your written request, as well as your name, email address, phone number, property address, and your account number. We may limit our response to your exercise of the above rights as permitted under applicable law. We will review each request carefully and respond accordingly within the timeframe established by the CCPA.

However, as discussed above, the CCPA does not apply to all or nearly all information we obtain, use, or share as part of our role as a financial institution or through certain business-to-business transactions, and we will not include any of that information in responding to your request.

Please note that we are not responsible for notices that are not labelled or sent properly, or that do not have complete information. If applicable, we will provide



you with information on how to submit the request or remedy any deficiencies with the request. Responses to your CCPA request will be delivered in the same manner that we received it.

Verifiable Request

As required under applicable law, we take steps to verify your identity before granting you access to information or acting on your request to exercise your rights. You must provide us with enough information to allow us to reasonably verify you are the person about whom we collected Personal Information, or an authorized representative, and describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it. Please include the statement “Attention: California Privacy Rights Request” in the body of your written request, as well as your name, email address, phone number, property address, and Community account number. We may limit our response to your exercise of the above rights as permitted under applicable law. We will review each request carefully and respond accordingly within the timeframe established by the CCPA.

Agent Authorization and Disability Access

You may designate an authorized agent to make a CCPA request for personal information on your behalf. To designate an authorized agent to act on your behalf, you must provide the agent with written permission to do so and provide proof of your identity. Written permission may include a power of attorney sufficient under California Probate Code §§ 4121 to 4130.

You may also make a verifiable consumer request on behalf of your minor child, but you must also provide proof that you are that child’s parent or legal guardian.

Other California Privacy Rights

California “Shine the Light” Law (Civil Code Section § 1798.83)

Under the Shine the Light Law, a California resident may ask us to refrain from sharing your Personal Information with third parties for their direct marketing purposes. Please know that we do not share Personal Information of California residents with third parties for their marketing purposes.



California Do Not Track Disclosure

Our website and applications are not designed to respond to “Do Not Track” requests from browsers.

Contact Information Regarding this California Notice

You may contact us with questions or concerns about our privacy policies or practices and your choices and rights under California law by writing us at Lakeview. Compliance Department, 4425 Ponce De Leon Boulevard, 5th Floor, Coral Gables, FL 33146 or email at privacy@lakeview.com. Reminder: please include the statement “Attention: California Privacy Rights Request” in the body of your written request, as well as your name, email address, phone number, property address, and your account number. Again, we may limit our response to your exercise of the above rights as permitted under applicable law. We will review each request carefully and respond accordingly within the timeframe established by the CCPA.

© Lakeview Loan Servicing, LLC. All rights reserved.

Lakeview Loan Servicing, LLC uses cookies on this website in order to improve and customize your browsing experiences and for analytics about our visitors. To accept cookies continue browsing or check the accept button below, please see our [Online Privacy Notice](#).

Accept

[Dismiss](#)

Cookie and Privacy Settings

How we use cookies

We may request cookies to be set on your device. We use cookies to let us know when you visit our websites, how you interact with us, to enrich your user experience, and to customize your relationship with our website.



Click on the different category headings to find out more. You can also change some of your preferences. Note that blocking some types of cookies may impact your experience on our websites and the services we are able to offer.

Essential Website Cookies

These cookies are strictly necessary to provide you with services available through our website and to use some of its features.

Because these cookies are strictly necessary to deliver the website, refusing them will have impact how our site functions. You always can block or delete cookies by changing your browser settings and force blocking all cookies on this website. But this will always prompt you to accept/refuse cookies when revisiting our site.

We fully respect if you want to refuse cookies but to avoid asking you again and again kindly allow us to store a cookie for that. You are free to opt out any time or opt in for other cookies to get a better experience. If you refuse cookies we will remove all set cookies in our domain.

We provide you with a list of stored cookies on your computer in our domain so you can check what we stored. Due to security reasons we are not able to show or modify cookies from other domains. You can check these in your browser security settings.

Other external services

We also use different external services like Google Webfonts, Google Maps, and external Video providers. Since these providers may collect personal data like your IP address we allow you to block them here. Please be aware that this might heavily reduce the functionality and appearance of our site. Changes will take effect once you reload the page.

Google Webfont Settings:



Google Map Settings:

Google reCaptcha Settings:

Vimeo and Youtube video embeds:

Privacy Policy

You can read about our cookies and privacy settings in detail on our Privacy Policy Page.



Exhibit “3”

Appendix

A security incident involving unauthorized access to Lakeview Loan Servicing, LLC's ("Lakeview") file servers was identified in early December 2021. Steps were immediately taken to contain the incident, notify law enforcement, and a forensic investigation firm was engaged. The investigation determined that an unauthorized person obtained access to files on Lakeview's file storage servers from October 27, 2021 to December 7, 2021. The accessed files were then reviewed by the investigation team to identify the content. On January 31, 2022, the review process generated a preliminary list of individuals, including Maine residents, whose name, address, loan number, and Social Security number were included in the files. After the initial file review process identified potential individuals to notify, Lakeview conducted extensive analysis and review of the draft list to work to develop the final list of individuals to notify, accounting for factors such as identifying the associated loan number to facilitate the ability to answer potential questions, identifying addresses, and overall review of the list to support timely and accurate notification. Lakeview also took steps to engage a third party to provide mailing, call center, and credit monitoring services.

On March 18, 2022, Lakeview will begin mailing notification letters via United States Postal Service First-Class mail to individuals whose information may have been involved, including to 9,511 Maine residents, in accordance with Me. Rev. Stat. Tit. 10, §1348. A copy of the notification letter is enclosed. Lakeview is offering eligible individuals complimentary one-year memberships in credit monitoring and identity protection services through Kroll. In addition, Lakeview has recommended that residents review their financial account statements and credit reports and report any unauthorized charges or activity and has established a dedicated, toll-free helpline where residents may obtain more information regarding the incident.

To prevent something like this from happening in the future, Lakeview has taken additional steps to further enhance its existing security measures.

LAKEVIEW LOAN SERVICING, LLC

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

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.

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 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. 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.

We wanted to notify you of this incident and assure you that we take it seriously. We engaged Kroll, a third party with monitoring expertise, to provide identity monitoring services at no cost to you for one year. The identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information on your complimentary one-year membership, as well as additional steps you can take in response to the incident, please see the additional information provided in this letter and visit info.krollmonitoring.com.

We regret that this incident occurred and apologize for any inconvenience. Additional steps are being taken to further enhance our existing security measures. If you have questions about this notice, please call (855) 541-3564 from 8:00 a.m. – 5:30 p.m. Central Time, Monday through Friday (excluding major US holidays).

Sincerely,



Judith Tribble
SVP, Chief Compliance Officer
Lakeview Loan Servicing, LLC



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves 8,118 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

Exhibit “4”

26204

LAKEVIEW LOAN SERVICING, LLC

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

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, including your 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. This notice explains measures we have taken and steps that you may consider taking.

We wanted to notify you of this incident and assure you that we take it seriously. We engaged Kroll, a third party with monitoring expertise, to provide identity monitoring services at no cost to you for two years. The identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information on your complimentary two-year membership, as well as additional steps you can take in response to the incident, please see the additional information provided in this letter and visit info.krollmonitoring.com.

We regret that this incident occurred and apologize for any inconvenience. Additional steps are being taken to further enhance our existing security measures. If you have questions about this notice, please call (855) 541-3564 from 8:00 a.m. – 5:30 p.m. Central Time, Monday through Friday (excluding major US holidays).

Sincerely,



Judith Tribble
SVP, Chief Compliance Officer
Lakeview Loan Servicing, LLC



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Exhibit “5”

LAKEVIEW LOAN SERVICING, LLC

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

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.

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 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. 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.

We wanted to notify you of this incident and assure you that we take it seriously. We engaged Kroll, a third party with monitoring expertise, to provide identity monitoring services at no cost to you for one year. The identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information on your complimentary one-year membership, as well as additional steps you can take in response to the incident, please see the additional information provided in this letter and visit info.krollmonitoring.com.

We regret that this incident occurred and apologize for any inconvenience. Additional steps are being taken to further enhance our existing security measures. If you have questions about this notice, please call (855) 541-3564 from 8:00 a.m. – 5:30 p.m. Central Time, Monday through Friday (excluding major US holidays).

Sincerely,



Judith Tribble
SVP, Chief Compliance Officer
Lakeview Loan Servicing, LLC



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves 8,118 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

Exhibit “6”



865 Howe Avenue, Sacramento, CA 95825
P: 916-777-7777 | F: 916-924-1829 | justice4you.com

CLAYEO C. ARNOLD
ANTHONY M. ONTIVEROS
JOHN T. STRALEN**
**Board-Certified Civil Trial
Advocate by National Board of
Trial Advocacy

M. ANDERSON BERRY
JOSHUA H. WATSON
ANDREW G. MINNEY
LIYA WALLACE
JEFFREY J.A. HINRICHSEN
GREGORY HAROUTUNIAN
ANTHONY J. POIDMORE*
GINA M. BOWDEN*
*Of Counsel

DATA BREACH
CLASS ACTION
QUI TAM
PERSONAL INJURY
WRONGFUL DEATH
EMPLOYMENT LAW
PRODUCT LIABILITY

April 14, 2022

VIA CERTIFIED MAIL

Pingora Loan Servicing, LLC
c/o Legal Department
1819 Wazee Street, 2nd Floor
Denver, CO 80202

USPS TRACKING # **9488 9090 0027 6006 4393 25**
SIG CON: FOR TRACKING GO TO USPS.COM

Pingora Loan Servicing, LLC
c/o Corporation Service Company- Registered Agent
1900 W. Littleton Boulevard
Littleton, CO 80120

USPS TRACKING # **9488 9090 0027 6006 4393 32**
SIG CON: FOR TRACKING GO TO USPS.COM

Bayview Asset Management, LLC
c/o Legal Department
4425 Ponce De Leon Boulevard, 5th Floor
Coral Gables, FL 33146

USPS TRACKING # **9488 9090 0027 6006 4393 49**
SIG CON: FOR TRACKING GO TO USPS.COM

Bayview Asset Management, LLC
c/o Brian E. Bombstein, Esq.- Registered Agent
4425 Ponce De Leon Boulevard, 5th Floor
Coral Gables, FL 33146

USPS TRACKING # **9488 9090 0027 6006 4393 56**
SIG CON: FOR TRACKING GO TO USPS.COM

RE: Statutory 30 Day Notice of Claim – Cal. Civil Code 1798.100, *et seq.*

This letter constitutes notice under the California Consumer Privacy Act (“CCPA”), California Civil Code section 1798.100, *et seq.* Pursuant to Civil Code section 1798.150(b), we are hereby notifying Pingora Loan Servicing, LLC (“Pingora”) and Bayview Asset Management, LLC (“Bayview” and collectively with Pingora, “Defendants”) that it has violated the CCPA, and we demand that, to the extent any cure exists, Defendants “actually cure[.]” such violation within thirty (30) calendar days from the date of this letter.

Our clients, Robert Keach, Maureen Keach, and Jay Saporta, residents of California, each received a Notice of Data Breach from Pingora on or about April 6, 2022, stating that their personally identifiable information (“PII”) was accessed and is no longer secure. The PII exposed includes, at least, name, address, loan number, and Social Security number. *See* CCPA § 1798.81.5(d)(1).

Please be advised that the failure to prevent Robert Keach’s, Maureen Keach’s, Jay Saporta’s and other California residents’ nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure, is a result of Defendants’ failure to meet their duty to implement and maintain reasonable security procedures and practices, which is a violation of Civil Code §§ 1798.81.5 and 1798.150. These failures include the lack of adequate encryption to sufficiently

Page 2
April 14, 2022

maintain California residents' PII and to protect this PII from being accessed by third parties without authorization.

To the extent there is any possible cure, we request that Defendants cure this violation which exposed Robert Keach's, Maureen Keach's, and Jay Saporta's PII, and provide an express written statement that the violations have been "actually cured" and that no further violations will occur. A cure, if possible, would require Defendants to, for example, recover all of the stolen PII and eliminate any future risk that Robert Keach's, Maureen Keach's, and Jay Saporta's stolen PII is accessed.

A failure to comply with this request within thirty (30) calendar days will subject Defendants to statutory damages on an individual and/or class-wide basis.

Thank you for your time and cooperation.

Very truly yours,

/s/M. Anderson Berry
M. Anderson Berry, Esq.
aberry@justice4you.com
916.239.4778

Exhibit “7”

BakerHostetler

Baker&Hostetler LLP

11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509

T 310.820.8800
F 310.820.8859
www.bakerlaw.com

Teresa C. Chow
direct dial: 310.979.8458
tchow@bakerlaw.com

April 29, 2022

CONFIDENTIAL

VIA E-MAIL (ABERRY@JUSTICE4YOU.COM)

M. Anderson Berry
Arnold Law Firm
865 Howe Avenue
Sacramento, CA 95825

Re: Pingora Loan Servicing, LLC ("Pingora") Response to Letter Dated April 14, 2022

Dear Anderson:

Baker & Hostetler LLP represents Pingora in connection with the data incident that occurred in 2021 (the "Incident"). We are in receipt of your letter dated April 14, 2022 (the "Letter") sent on behalf of your clients, Robert Keach, Maureen Keach, and Jay Saporta, purporting to provide notice pursuant to the California Consumer Privacy Act ("CCPA"). Although your clients have not perfected any claim for statutory damages under the CCPA, and we deny that they suffered any such damages, we nonetheless hereby provide the following express written statement pursuant to California Civil Code § 1798.150(b) that any alleged violation of the CCPA has been cured.

I. THE LETTER FAILS TO COMPLY WITH CAL. CIV. CODE § 1798.150(b).

The Letter fails to comply with the requirements of Section 1798.150(b). That section requires a notice "identifying the specific provisions of this title the consumer alleges have been or are being violated." The Letter simply contains generic references to Section 1798.81.5, which sets forth the Legislature's intent, and Section 1798.150, which governs when a private right of action exists. You have not identified any specific provision of the CCPA that you contend Pingora violated. The general allegations regarding Pingora's alleged "failure to meet their duty to implement and maintain reasonable security procedures and practices" and "lack of adequate encryption," which Pingora disputes, are not tied to a violation of any particular provision of the CCPA. Without waiving our objection to these deficiencies, we nevertheless provide the following response.

April 29, 2022

Page 2

II. PINGORA CURED ANY ALLEGED CCPA VIOLATION.

When the incident was detected, containment measures were implemented that terminated the unauthorized access. A thorough investigation was conducted. The containment measures terminated the unauthorized access and included: installation of firewall blocks of IP addresses; secure removal of files installed during the incident; deployment of an additional endpoint threat detection and response tool (FireEye HX) with 24/7 monitoring by Mandiant; and a global password reset, including service accounts and Kerberos ticket. The investigation did not identify any unauthorized access after December 7, 2021, the date containment measures were initiated. The FBI and Secret Service were notified. Actions were also taken to reduce files that the threat actor had access to.

Additional enhanced security measures were implemented, including: network segmentation to further restrict access to file servers and shared folders; more rigid protocols for decision-making during review of alerts from endpoint threat detection and response tools by the managed security operations center and security team; enhanced logging practices to have additional data sent to the security information and event management application for analysis; establishment of network traffic baselines to support monitoring of egress traffic for anomalous events; and implementation of a solution to prevent/control web downloads. Pingora also mailed notification letters to individuals to inform them of the Incident, and the letter included information on how to enroll in an identity and credit monitoring service that Pingora paid for Kroll to provide.

Pingora disputes that the procedures and practices in place at the time of the Incident were unreasonable. Layers of security measures that included technical and administrative safeguards had been implemented. Nevertheless, for all the reasons stated above, this letter constitutes an express written statement that any alleged CCPA violations have been cured and no further violations shall occur. Specifically, Pingora has cured any “security procedures and practices” that you could possibly claim were unreasonable at the time of the incident.

We appreciate your attention to this matter. To the extent you would like to discuss any of the above, please feel free to contact me at any time.

Sincerely,

/s/ Teresa C. Chow

Teresa C. Chow
Baker & Hostetler LLP

BakerHostetler

Baker&Hostetler LLP

11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509

T 310.820.8800
F 310.820.8859
www.bakerlaw.com

Teresa C. Chow
direct dial: 310.979.8458
tchow@bakerlaw.com

April 29, 2022

CONFIDENTIAL

VIA E-MAIL (AK@KAZLG.COM)

Abbas Kazerounian
KAZEROUNI LAW GROUP, APC
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626

Re: Lakeview Loan Servicing, LLC ("Lakeview") Response to Letter Dated April 13, 2022

Dear Abbas:

Baker & Hostetler LLP represents Lakeview in connection with the data incident that occurred in 2021 (the "Incident"). We are in receipt of your letter dated April 13, 2022 (the "Letter") sent on behalf of your client, Pedro Rubio, purporting to provide notice pursuant to the California Consumer Privacy Act ("CCPA"). Although your client has not perfected any claim for statutory damages under the CCPA, and we deny that he suffered any such damages, we nonetheless hereby provide the following express written statement pursuant to California Civil Code § 1798.150(b) that any alleged violation of the CCPA has been cured.

I. THE LETTER FAILS TO COMPLY WITH CAL. CIV. CODE § 1798.150(b).

The Letter fails to comply with the requirements of Section 1798.150(b). That section requires a notice "identifying the specific provisions of this title the consumer alleges have been or are being violated." The Letter simply contains generic references to Section 1798.81.5, which sets forth the Legislature's intent, and Section 1798.150, which governs when a private right of action exists. You have not identified any specific provision of the CCPA that you contend Lakeview violated. The sole general allegation that Lakeview "fail[ed] to provide reasonable security," which Lakeview disputes, is not tied to a violation of any particular provision of the CCPA. Without waiving our objection to these deficiencies, we nevertheless provide the following response.

II. LAKEVIEW CURED ANY ALLEGED CCPA VIOLATION.

When the incident was detected, containment measures were implemented that terminated the unauthorized access. A thorough investigation was conducted. The containment measures

April 29, 2022

Page 2

terminated the unauthorized access and included: installation of firewall blocks of IP addresses; secure removal of files installed during the incident; deployment of an additional endpoint threat detection and response tool (FireEye HX) with 24/7 monitoring by Mandiant; and a global password reset, including service accounts and Kerberos ticket. The investigation did not identify any unauthorized access after December 7, 2021, the date containment measures were initiated. The FBI and Secret Service were notified. Actions were also taken to reduce files that the threat actor had access to.

Additional enhanced security measures were implemented, including: network segmentation to further restrict access to file servers and shared folders; more rigid protocols for decision-making during review of alerts from endpoint threat detection and response tools by the managed security operations center and security team; enhanced logging practices to have additional data sent to the security information and event management application for analysis; establishment of network traffic baselines to support monitoring of egress traffic for anomalous events; and implementation of a solution to prevent/control web downloads. Lakeview also mailed notification letters to individuals to inform them of the Incident, and the letter included information on how to enroll in an identity and credit monitoring service that Lakeview paid for Kroll to provide.

Lakeview disputes that the procedures and practices in place at the time of the Incident were unreasonable. Layers of security measures that included technical and administrative safeguards had been implemented. Nevertheless, for all the reasons stated above, this letter constitutes an express written statement that any alleged CCPA violations have been cured and no further violations shall occur. Specifically, Lakeview has cured any “security procedures and practices” that you could possibly claim were unreasonable at the time of the incident.

We appreciate your attention to this matter. To the extent you would like to discuss any of the above, please feel free to contact me at any time.

Sincerely,

/s/ Teresa C. Chow

Teresa C. Chow
Baker & Hostetler LLP

BakerHostetler

Baker&Hostetler LLP

11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509

T 310.820.8800
F 310.820.8859
www.bakerlaw.com

Teresa C. Chow
direct dial: 310.979.8458
tchow@bakerlaw.com

November 10, 2022

CONFIDENTIAL

VIA E-MAIL (ABERRY@JUSTICE4YOU.COM)

M. Anderson Berry
865 Howe Avenue
Sacramento, CA 95825

Re: Community Loan Servicing, LLC and Bayview Asset Management, LLC Response to Letter Dated October 31, 2022

Dear Mr. Berry:

Baker & Hostetler LLP represents Community Loan Servicing, LLC (“Community”) and Bayview Asset Management, LLC (“Bayview”) in connection with the data security incident that occurred in 2021 (the “Incident”). We are in receipt of your letter dated October 31, 2022 (the “Letter”) sent on behalf of your client, Linda Kim, purporting to provide notice pursuant to the California Consumer Privacy Act (“CCPA”). Although your client has not perfected any claim for statutory damages under the CCPA, and we deny that she suffered any such damages, we nonetheless hereby provide the following express written statement pursuant to California Civil Code § 1798.150(b) that any alleged violation of the CCPA has been cured.

I. THE LETTER FAILS TO COMPLY WITH CAL. CIV. CODE § 1798.150(b).

The Letter fails to comply with the requirements of Section 1798.150(b). That section requires a notice “identifying the specific provisions of this title the consumer alleges have been or are being violated.” The Letter simply contains generic references to Section 1798.81.5 and Section 1798.150, which governs when a private right of action exists. You have not identified any specific provision of the CCPA that you contend Lakeview violated. The general allegations regarding Lakeview’s alleged “lack of adequate encryption to sufficiently maintain California residents’ PII and to protect this PII from being accessed by third parties without authorization,” which Community and Bayview dispute, are not tied to a violation of any particular provision of the CCPA. Without waiving Community and Bayview’s objection to these deficiencies, we nevertheless provide the following response.

November 10, 2022

Page 2

II. COMMUNITY AND BAYVIEW CURED ANY ALLEGED CCPA VIOLATION.

When the incident was detected, containment measures were implemented that terminated the unauthorized access. A thorough investigation was conducted. The containment measures terminated the unauthorized access and included: installation of firewall blocks of IP addresses; secure removal of files installed during the incident; deployment of an additional endpoint threat detection and response tool (FireEye HX) with 24/7 monitoring by Mandiant; and a global password reset, including service accounts and Kerberos ticket. The investigation did not identify any unauthorized access after December 7, 2021, the date containment measures were initiated. The FBI and Secret Service were notified. Actions were also taken to reduce files that the threat actor had access to.

Additional enhanced security measures were implemented, including: network segmentation to further restrict access to file servers and shared folders; more rigid protocols for decision-making during review of alerts from endpoint threat detection and response tools by the managed security operations center and security team; enhanced logging practices to have additional data sent to the security information and event management application for analysis; establishment of network traffic baselines to support monitoring of egress traffic for anomalous events; and implementation of a solution to prevent/control web downloads. Community also mailed notification letters to individuals to inform them of the Incident, and the letters included information on how to enroll in an identity and credit monitoring service that Community paid for Kroll to provide.

Community and Bayview dispute that the procedures and practices in place at the time of the Incident were unreasonable. Layers of security measures that included technical and administrative safeguards had been implemented. Nevertheless, for all the reasons stated above, this letter constitutes an express written statement that any alleged CCPA violations have been cured and no further violations shall occur. Specifically, Community and Bayview have cured any “security procedures and practices” that you could possibly claim were unreasonable at the time of the incident.

We appreciate your attention to this matter. To the extent you would like to discuss any of the above, please feel free to contact me at any time.

Sincerely,

/s/ Teresa C. Chow

Teresa C. Chow
Baker & Hostetler LLP

Exhibit “8”



(213) 444-1973 (213) 457-3092 jon@lebelaw.com 777 S. Alameda Street, 2nd Floor, Los Angeles, CA 90021

April 29, 2022

VIA CERTIFIED U.S. MAIL WITH RETURN RECEIPT

Lakeview Loan Servicing, LLC
4425 Ponce De Leon Blvd., Fifth Floor
Coral Gables, FL 33146

Re: Notice under California Civil Code section 1798.150 of the California Consumer Privacy Act (“CCPA”) by Cindy Villanueva on Behalf of Herself and All Others Similarly Situated

Dear Lakeview Loan Servicing, LLC,

Please be advised that Cindy Villanueva has retained Lebe Law, A Professional Law Corporation to represent her individually, and on behalf of all others similarly situated, to address the unauthorized data disclosure by Lakeview Loan Servicing, LLC, that was announced in a notice you provided to Ms. Villanueva on approximately March 17, 2022, as a result of an unauthorized party accessing your file storage servers during the time period of October 27, 2021 to December 7, 2021.

In violation of California Civil Code section 1798.150(a)(1), Lakeview Loan Servicing, LLC subjected Cindy Villanueva and all others similarly situated to “an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.”

“All others similarly situated” is defined as follows: All persons in the United States whose personal information was accessed, compromised, or stolen as a result of the data breach announced by Lakeview Loan Servicing, LLC on or about March 17, 2022.

This letter shall constitute notice under California Civil Code section 1798.150 of the CCPA that Cindy Villanueva, individually and on behalf of all others similarly situated,

demands that you remedy the violations of the CCPA within thirty (30) days from your receipt of this letter.

It is the contention of Ms. Villanueva, on behalf of herself and all others similarly situated, that you violated subsection (a) Civil Code section 1798.150, which reads as follows:

(a)(1) Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

- (A) To recover damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater.
- (B) Injunctive or declaratory relief.
- (C) Any other relief the court deems proper.

Ms. Villanueva, individually and on behalf of all other similarly situated, hereby requests that Lakeview Loan Servicing, LLC cure this unauthorized data disclosure and any resulting harm to the personal information ("PI") implicated in the breach. The cure to this data breach must occur within thirty (30) days from the date of this correspondence.

We solicit your prompt attention to this matter and thank you in advance for your anticipated cooperation. Should you have any questions, please feel free to contact me at your convenience.

Sincerely,

A handwritten signature in black ink, appearing to be 'J. Lebe', with a stylized flourish at the end.

Jonathan M. Lebe, Esq.
Attorney for Cindy Villanueva,
Individually and on behalf of all other similarly situated

Exhibit “9”



245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
www.kazlg.com

April 13, 2022

VIA CERTIFIED MAIL

Lakeview Loan Servicing, LLC
4425 Ponce De Leon Boulevard, 5th Floor
Coral Gables, Florida 33146.

Re: Rubio v. Lakeview Loan Servicing, LLC

To Whom It May Concern:

We represent Plaintiff Pedro Rubio ("Plaintiff") and all other similarly situated consumers in a putative class action against Lakeview Loan Servicing, LLC ("Defendant") arising out of, *inter alia*, Defendant's failure to provide reasonable security for Plaintiff's and the proposed class members' personal information, which resulted in the unauthorized access, theft, or disclosure of this information (the "Data Breach"). To our knowledge the Data Breach occurred on between October 27, 2021 to December 7, 2021, as specified in Defendant's "Notice of Data Breach" letter dated March 17, 2022.

The full claims, including the facts and circumstances surrounding these claims are detailed in Plaintiff's Class Action Complaint, a copy of which is attached and incorporated by reference. Defendant's conduct constitutes violations of California Civil Code §§ 1798.81.5(a)(1) and 1798.150(a)(1) among other consumer protection statutes.

While this letter and the attached Complaint constitute sufficient notice of the claims asserted against Defendant, pursuant to California Civil Code 1798.150(b)(1), Plaintiff demands that, in the event a cure is possible, Defendant is hereby provided the opportunity to actually cure the noticed violations and provide Plaintiff with an express written statement within thirty (30) days that the violations have been cured and that no further violations shall occur. A cure, if possible, requires that all the information taken has been recovered and that Plaintiff and the proposed class members of similarly situated persons are not at any risk of any of the information being used.

Thank you for your time and attention to this matter.

Sincerely,

s/ Abbas Kazerounian

Abbas Kazerounian, Esq.
KAZEROUNI LAW GROUP, APC
Direct Line: (800) 400-6808, Ext. 2
E-mail: ak@kazlg.com

[Enclosure]

KAZEROUNI LAW GROUP, APC
Abbas Kazerounian, Esq. (SBN: 249203)
ak@kazlg.com
Mona Amini, Esq. (SBN: 296829)
mona@kazlg.com
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523

Attorneys for Plaintiff
Pedro Rubio and the putative class

SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF RIVERSIDE – COMPLEX CIVIL

PEDRO RUBIO, individually and on behalf of all
others similarly situated,

Plaintiff,

vs.

LAKEVIEW LOAN SERVICING, LLC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT FOR
VIOLATIONS OF:

1. CALIFORNIA CONSUMER PRIVACY
ACT OF 2018, CAL. CIV. CODE §§
1798.100, *et seq.*;
2. CALIFORNIA UNFAIR COMPETITION
LAW, CAL. BUS. & PROF. CODE
§§ 17200, *et seq.*; and
3. BREACH OF CONTRACT

DEMAND FOR JURY TRIAL

//

//

//

//

//

//

//

Plaintiff PEDRO RUBIO (“Plaintiff”), individually and on behalf of himself and the general public and all others similarly situated (“Class members”), by and through his attorneys, upon personal knowledge as to facts pertaining to himself and on information and belief as to all other matters, brings this class action against Defendant LAKEVIEW LOAN SERVICING, LLC (“Defendant” or “Lakeview”), and alleges as follows:

NATURE OF THE CASE

1. This is a data breach class action against Defendant and its related entities, subsidiaries, and agents for failing to secure and safeguard the personally identifiable information (“PII”) that Defendant collected and maintained and for failing to provide timely and adequate notice to Plaintiff and other Class members that their information had been stolen. Lakeview Loan Servicing, LLC is the fourth-largest mortgage service company in the United States and services mortgages, holds escrow, and provides customer service for over 1.5 million homeowners nationwide. For its business purposes, Defendant collects, receives, and maintains a substantial amount of PII from homeowners, like Plaintiff, in its servers and/or networks.

2. On or about March 17, 2022, Defendant issued a Notice of Data Breach letter announcing that there had been unauthorized access to its file servers which was identified in early December 2021, and it determined that an unauthorized person obtained access to its file storage servers from October 27, 2021 to December 7, 2021. (the “Data Breach”). Defendant conducted a review of the files that were accessed in the Data Breach and on January 31, 2022, its review process determined files containing Plaintiff’s and other similarly situated individuals’ PII, including names, addresses, loan account numbers, and Social Security numbers, were included in the files accessed and/or obtained in the Data Breach. The Notice of Data Breach letter further indicated that the accessed files may also have included information provided in connection with a loan application, loan modification, or other items regarding loan servicing.

3. Although the Data Breach was identified in December 2021, placing sensitive customer information in the hands of malicious actors as a result of Defendant’s failure to safeguard Plaintiff’s and others’ PII, Defendant waited several months until on or around March 17, 2022 to provide the Notice of Data Breach to Plaintiff and other similarly situated customers. This notice



1 was still lacking in information necessary for Plaintiff and Class members to understand the scope
2 and severity of the Data Breach. Due to this lapse in time between the Data Breach and Defendant's
3 notice to affected customers, unauthorized third parties have already been able to acquire and sell
4 Plaintiff's and the Class members' PII on the black market or dark web, or otherwise fraudulently
5 misuse it for their personal gain.

6 4. Defendant owed a duty to Plaintiff and Class members to implement and maintain
7 reasonable and adequate security measures to secure, protect, and safeguard the PII it collected from
8 its customers and maintained for business purposes and stored on its networks.

9 5. Defendant breached that duty by, *inter alia*, failing to implement and maintain
10 reasonable security procedures and practices to protect PII from unauthorized access and storing
11 and retaining Plaintiff's and Class members' personal information on inadequately protected servers
12 and/or networks.

13 6. The Data Breach happened because of Defendant's inadequate cybersecurity, which
14 caused Plaintiff's and Class members' PII to be accessed, viewed, stolen and/or disclosed to
15 unauthorized persons. This action seeks to remedy these failings. Plaintiff brings this action on
16 behalf of himself individually and on behalf of all other similarly situated California residents
17 affected by the Data Breach.

18 7. As set forth in the Prayer for Relief, among other things, Plaintiff seeks, for himself
19 and the Class, equitable relief, including public injunctive relief, and actual damages.

20 **VENUE AND JURISDICTION**

21 8. This Court has jurisdiction over this action pursuant to Cal. Code Civ. Proc. § 410.10
22 and Cal. Bus. & Prof. Code §§ 17203-17204, 17604. This action is brought as a class action on
23 behalf of Plaintiff and Class members pursuant to Cal. Code Civ. Proc. § 382.

24 9. This Court has personal jurisdiction over Defendant because Defendant's regularly
25 conducts business in California and with California consumers.

26 10. Venue is proper in this Court pursuant to Cal. Code Civ. Proc. §§ 395 and 395.5
27 because Defendant regularly conducts business in this county, and unlawful acts or omissions have
28 occurred in this county.

PARTIES

11. At all relevant times, Plaintiff resided in Riverside County, California. Plaintiff is a homeowner whose mortgage was serviced by Defendant and had his personal information and PII collected and maintained by Defendant.

12. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information it collected and maintained, Plaintiff's PII accessed, exfiltrated, viewed, stolen and/or disclosed to unauthorized persons in the Data Breach.

13. Defendant is a limited liability company formed under the laws of the state of Delaware with its principal place of business and/or headquarters located at 4425 Ponce De Leon Boulevard, 5th Floor, Coral Gables, Florida 33146.

FACTUAL ALLEGATIONS***PII Is a Valuable Property Right that Must Be Protected***

14. The California Constitution guarantees every Californian a right to privacy. And PII is a recognized valuable property right.¹ California has repeatedly recognized this property right, most recently with the passage of the California Consumer Privacy Act of 2018.

15. In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by observing:

Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.²

16. The value of PII as a commodity is measurable. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of

¹ See John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *2 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

² FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), <https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable>.

1 traditional financial assets.”³ It is so valuable to identity thieves that once PII has been disclosed,
2 criminals often trade it on the “cyber black-market” for several years.

3 17. Companies recognize PII as an extremely valuable commodity akin to a form of
4 personal property. For example, Symantec Corporation’s Norton brand has created a software
5 application that values a person’s identity on the black market.⁴

6 18. As a result of its real value and the recent large-scale data breaches, identity thieves
7 and cyber criminals openly post credit card numbers, Social Security numbers, PII and other
8 sensitive information directly on various illicit Internet websites making the information publicly
9 available for other criminals to take and use. This information from various breaches, including the
10 information exposed in the Data Breach, can be aggregated and become more valuable to thieves
11 and more damaging to victims. In one study, researchers found hundreds of websites displaying
12 stolen PII and other sensitive information. Strikingly, none of these websites were blocked by
13 Google’s safeguard filtering mechanism – the “Safe Browsing list.”

14 19. Recognizing the high value that consumers place on their PII, some companies now
15 offer consumers an opportunity to sell this information to advertisers and other third parties. The
16 idea is to give consumers more power and control over the type of information they share – and
17 who ultimately receives that information. By making the transaction transparent, consumers will
18 make a profit from the surrender of their PII.⁵ This business has created a new market for the sale
19 and purchase of this valuable data.⁶

20 20. Consumers place a high value not only on their PII, but also on the privacy of that
21 data. Researchers shed light on how much consumers value their data privacy – and the amount is
22 considerable. Indeed, studies confirm that “when privacy information is made more salient and
23

24
25 ³ See Soma, *Corporate Privacy Trend*, *supra*.

26 ⁴ Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

27 ⁵ Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010)
available at <https://www.nytimes.com/2010/07/18/business/18unboxed.html>.

28 ⁶ See Julia Angwin and Emil Steel, *Web’s Hot New Commodity: Privacy*, Wall Street Journal
(Feb. 28, 2011) available at <https://www.wsj.com/articles/SB10001424052748703529004576160764037920274>.

1 accessible, some consumers are willing to pay a premium to purchase from privacy protective
2 websites.”⁷

3 21. One study on website privacy determined that U.S. consumers valued the restriction
4 of improper access to their PII between \$11.33 and \$16.58 per website.⁸

5 22. Given these facts, any company that transacts business with a consumer and then
6 compromises the privacy of consumers’ PII has thus deprived that consumer of the full monetary
7 value of the consumer’s transaction with the company.

8 ***Theft of PII Has Grave and Lasting Consequences for Victims***

9 23. A data breach is an incident in which sensitive, protected, or confidential data has
10 potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers
11 rely on the internet and apps on their phone and other devices to conduct every-day transactions,
12 data breaches are becoming increasingly more harmful.

13 24. Theft or breach of PII is serious. The California Attorney General recognizes that
14 “[f]oundational” to every Californian’s constitutional right to privacy is “information security: if
15 companies collect consumers’ personal data, they have a duty to secure it. An organization cannot
16 protect people’s privacy without being able to secure their data from unauthorized access.”⁹

17 25. The United States Government Accountability Office noted in a June 2007 report on
18 Data Breaches (“GAO Report”) that identity thieves use PII to take over existing financial accounts,
19 open new financial accounts, receive government benefits and incur charges and credit in a person’s
20 name.¹⁰ As the GAO Report states, this type of identity theft is so harmful because it may take time
21 for the victim to become aware of the theft and can adversely impact the victim’s credit rating.

22
23
24
25 ⁷ Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An*
26 *Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), available at
27 <https://www.jstor.org/stable/23015560?seq=1#>

28 ⁸ II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation*
(Mar. 2003) at table 3, available at <https://ideas.repec.org/p/wpa/wuwpio/0304001.html> (emphasis
added).

⁹ California Data Breach Report, Kamala D. Harris, Attorney General, California Department
of Justice, February 2016.

¹⁰ See GAO, GAO Report 9 (2007) available at <http://www.gao.gov/new.items/d07737.pdf>.



26. In addition, the GAO Report states that victims of identity theft will face “substantial costs and inconveniences repairing damage to their credit records ... [and their] good name.” According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.¹¹

27. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.¹² According to Experian, “[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it” to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver’s license or ID; use the victim’s information in the event of arrest or court action.¹³

28. 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

¹¹ See FTC Identity Theft Website: <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>.

¹² The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 16 C.F.R. § 603.2. 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.” *Id.*

¹³ See Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), available at <https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/>.

your Social Security number and assuming your identity can cause a lot of problems.¹⁴

29. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was \$150 per record.¹⁵ Other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was \$298 dollars.¹⁶ And in 2019, Javelin Strategy & Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was \$375.¹⁷

30. A person whose PII has been compromised may not see any signs of identity theft for years. According to the GAO Report:

"[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. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.¹⁸

32. It is within this context that Plaintiff and thousands of similar homeowners must now live with the knowledge that their PII is forever in cyberspace and was taken by unauthorized persons willing to use the information for any number of improper purposes and scams, including making the information available for sale on the dark web and/or the black market.

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>.

¹⁵ Brook, *What's the Cost of a Data Breach in 2019*, *supra*.

¹⁶ Norton By Symantec, 2013 Norton Report 8 (2013), *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

¹⁷ Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, *available at* <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (citing the Javelin report).

¹⁸ See Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), *available at* <https://blog.linkedin.com/2016/05/18/protecting-our-members>.

Defendant's Collection of Customers' PII

33. Defendant represents that it understands the importance of protecting such information. For example, in its Online Privacy Policy, Defendant states that it “respects your privacy” and “recognizes the importance of keeping the personal information you provide to us private and secure,” and that it “use[s] the latest technology to ensure that your personal information is secure.”¹⁹

34. Defendant further represents that it maintains “commercially reasonable security measures to protect the personal information we collect and store from loss, misuse, destruction, or unauthorized access. Our security includes physical, administrative, and technology-based measures. We use industry-standard encryption to protect data in transit and at rest. Our internal policies and procedures impose a number of standards to safeguard the confidentiality of personal information, prohibit the unlawful disclosure of personal information, and limit access to personal information.”²⁰

35. Defendant’s Privacy Policy states, “The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- Social Security number and income
- Account balances and payment history
- Credit history and credit scores.”²¹

36. The types of information Defendant collects are further detailed in its Online Privacy Policy,²² which for California customers, identifies the categories of personal information it may have collected about them over the past 12 months as part of the mortgage origination process, which was then provided to Lakeview when it became their mortgage servicer, or information Lakeview received from third parties in connection with processing, underwriting, funding, and servicing their loan. Lakeview states this information is necessary for it to complete mortgage loan

¹⁹ See Lakeview’s Online Privacy Notice: <https://lakeview.com/privacy-notice/>

²⁰ *Id.*

²¹ See Lakeview’s Privacy Policy: <https://lakeview.com/privacy-policy/>

²² See Lakeview’s Online Privacy Notice: <https://lakeview.com/privacy-notice/>



1 transaction or transact as a mortgage servicer in accordance with federal and state law. and which
2 information is covered by the California Consumer Privacy Act (“CCPA”), including:

- 3 • Identifiers such as real name, alias, postal address, email address, IP address,
4 unique personal identifier, online identifier, account name, social security
5 number, and driver’s license number, passport number or other government
6 issued number, when you submit this information to create an account, apply for
7 a loan, request to learn more about our financial products and services, or
8 subscribe to email alerts.
- 9 • Any information that identifies, relates to, describes, or is capable of being
10 associated with a particular consumer or household, including, the “identifiers”
11 listed in (A), and the following: signature, insurance policy number,
12 employment, employment history, bank account number, credit card number,
13 debit card number, or any other financial information when you apply for or
14 receive a loan which was then provided to us when we became your master
15 servicer.
- 16 • The following categories of protected classification characteristics under
17 California or federal law: date of birth/age (40 years or older), gender, race,
18 color, national origin, citizenship, or marital status, when you provide it to us.
- 19 • Internet or other similar network activity information, including, but not limited
20 to, browsing history on our websites, search history, and information on your
21 interaction with our websites or applications when you choose to visit and
22 interact with our websites or applications.
- 23 • Audio information such as recordings of when you called into our customer
24 contact line; visual images from security cameras in our branch offices; and
25 electronic information in the form of Internet or other electronic network activity
26 information, as described above.
- 27 • Current or past professional or employment-related information, including job
28 history, performance evaluations, position details, or references.

The Data Breach

37. On or around March 17, 2022, Defendant issued an official Notice of Data Breach to
Plaintiff and its other homeowners who were victims of the Data Breach stating, “[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
investigation firm was engaged.”

38. According to Defendant, its “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. On January 31,
2022, the review process generated a preliminary list of individuals, including you, whose name,



1 address, loan number, and Social Security number were included in the files. We then took
2 extensive measures to review that list to ensure accuracy and prepare the list to be used to mail
3 notification letters. For some, the accessed files may also have included information provided in
4 connection with a loan application, loan modification, or other items regarding loan servicing.”

5 39. Defendant’s Notice of Data Breach letter provided little other information regarding
6 the Data Breach itself. For instance, Defendant provided no information regarding why it waited
7 months since learning of the data breach and identifying Plaintiff and other affected homeowners to
8 send them notice or how many people were affected by the Data Breach.

9 40. Reportedly, **2,537,261 individuals** were affected by the Data Breach.²³

10 41. As a result of the Data Breach, Plaintiff has suffered an invasion and loss of
11 Plaintiff’s privacy, and Plaintiff has spent additional time monitoring Plaintiff’s personal financial
12 accounts, which was time that Plaintiff otherwise would have spent performing other activities or
13 leisurely events for the enjoyment of life rather than mitigating the impact of the Data Breach.

14 42. As a result of the Data Breach, Plaintiff is and will continue to be at heightened risk
15 for financial fraud, mortgage fraud, and/or identity theft, and the associated damages resulting from
16 it, for years to come.

17 ***Defendant Knew or Should Have Known PII Are High Risk Targets***

18 43. Defendant knew or should have known that PII like that at issue here, is a high-risk
19 target for identity thieves.

20 44. The Identity Theft Resource Center reported that the banking/credit/financial sector
21 had the third largest number of breaches in 2018. According to the ITRC this sector suffered 135
22 data breaches exposing at least 1,709,013 million records in 2018.²⁴

23 45. Prior to the breach there were many reports of high-profile data breaches that should
24 have put a company like Defendant on high alert and forced it to closely examine its own security
25

26
27 ²³ See Office of the Maine Attorney General’s website:
<https://apps.web.maine.gov/online/aeviewer/ME/40/3d0c184e-e78c-4123-8ce8-8535f71facd3.shtml>

28 ²⁴ Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, available at
https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

1 procedures, as well as those of third parties with which it did business and gave access to its
2 subscriber PII. Notable breaches included Capital One, which announced that in March 2019 a
3 hacker had gained access to 100 million U.S. customer accounts and credit card applications.
4 Similarly, in May 2019, First American Financial reported a security incident on its website that
5 potentially exposed 885 million real estate and mortgage related documents, among others. Across
6 industries, financial services have the second-highest cost per breached record, behind healthcare. In
7 financial services, an average breach costs \$210 per record, while a “mega breach,” like Capital
8 One’s, can cost up to \$388 per record.²⁵

9 46. Anurag Kahol, CTO of Bitglass recently commented that “[g]iven that organizations
10 in the financial services industry are entrusted with highly valuable, personally identifiable
11 information (PII), they represent an attractive target for cybercriminals[.]” HelpNetSecurity reports
12 that “[h]acking and malware are leading the charge against financial services and the costs
13 associated with breaches are growing. Financial services organizations must get a handle on data
14 breaches and adopt a proactive security strategy if they are to properly protect data from an
15 evolving variety of threats.”²⁶

16 47. As such, Defendant was aware that PII is at high risk of theft, and consequently
17 should have but did not take appropriate and standard measures to protect Plaintiff’s and Class
18 members’ PII against cyber-security attacks that Defendant should have anticipated and guarded
19 against.

20 CLASS ACTION ALLEGATIONS

21 48. Pursuant to Cal. Code Civ. Proc. § 382 and Cal. Civ. Code § 1781, Plaintiff seeks to
22 represent and intends to seek certification of a class (the “Class”) defined as:

23 ***All California residents whose PII was subjected to the Data Breach.***
24

25
26 ²⁵ Samantha Ann Schwartz, 62% of breached data came from financial services in 2019,
27 CioDive (Dec. 23, 2019), available at <https://www.ciodive.com/news/62-of-breached-data-came-from-financial-services-in-2019/569592/>.

28 ²⁶ HelpNetSecurity, *Hacking and malware cause 75% of all data breaches in the financial services industry* (Dec. 17, 2019), available at <https://www.helpnetsecurity.com/2019/12/17/data-breaches-financial-services/>.



1 49. Excluded from the Class are: (1) Defendant and its officers, directors, employees,
2 principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents,
3 affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such
4 persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of
5 their immediate families.

6 50. Certification of Plaintiff's claims for class wide treatment is appropriate because
7 Plaintiff can prove the elements of their claims on a class wide basis using the same evidence as
8 would be used to prove those elements in individual actions alleging the same claims.

9 51. The Class members are so numerous and geographically dispersed throughout
10 California that joinder of all Class members would be impracticable. While the exact number of
11 Class members is unknown, **the Data Breach reportedly affected 2,537,261 persons**, Defendant
12 acknowledges the Data Breach, and based on information and belief, the Class consists of tens of
13 thousands of Defendant's customers in California, including Plaintiff and the Class members.
14 Plaintiff therefore believes that the Class is so numerous that joinder of all members is impractical.

15 52. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed
16 members of the Class, had their PII compromised in the Data Breach. Plaintiff and Class members
17 were injured by the same wrongful acts, practices, and omissions committed by Defendant, as
18 described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that
19 give rise to the claims of all Class members.

20 53. There is a well-defined community of interest in the common questions of law and
21 fact affecting Class members. The questions of law and fact common to Class members
22 predominate over questions affecting only individual Class members, and include without
23 limitation:

24 (a) Whether Defendant had a duty to implement and maintain reasonable security
25 procedures and practices appropriate to the nature of the PII it collected, stored,
26 and maintained from Plaintiff and Class members;

27 (b) Whether Defendant breached its duty to protect the PII of Plaintiff and each Class
28 member; and

(c) Whether Plaintiff and each Class member are entitled to damages and other equitable relief.

54. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that Plaintiff has no interests adverse to or that conflicts with the Class Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

55. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class are outweighed by the costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

56. Defendant has acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final injunctive, including public injunctive relief, and declaratory relief with respect to the Class as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the California Consumer Privacy Act of 2018 (“CCPA”) Cal. Civ. Code §§ 1798.100, *et seq.*

57. Plaintiff reallege and incorporates by reference all proceeding paragraphs as if fully set forth herein.

58. As more personal information about consumers is collected by businesses, consumers’ ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately



1 protect it from unauthorized access. The California Legislature explained: “The unauthorized
2 disclosure of personal information and the loss of privacy can have devastating effects for individuals,
3 ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to
4 destruction of property, harassment, reputational damage, emotional stress, and even potential
5 physical harm.”²⁷

6 59. As a result, in 2018, the California Legislature passed the CCPA, giving consumers
7 broad protections and rights intended to safeguard their personal information. Among other things,
8 the CCPA imposes an affirmative duty on businesses that maintain personal information about
9 California residents to implement and maintain reasonable security procedures and practices that are
10 appropriate to the nature of the information collected. Defendant failed to implement such
11 procedures which resulted in the Data Breach.

12 60. It also requires “[a] business that discloses personal information about a California
13 resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the
14 third party implement and maintain reasonable security procedures and practices appropriate to the
15 nature of the information, to protect the personal information from unauthorized access, destruction,
16 use, modification, or disclosure.” 1798.81.5(c).

17 61. Section 1798.150(a)(1) of the CCPA provides: “Any consumer whose nonencrypted
18 or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access
19 and exfiltration, theft, or disclosure as a result of the business’ violation of the duty to implement
20 and maintain reasonable security procedures and practices appropriate to the nature of the
21 information to protect the personal information may institute a civil action for” statutory or actual
22 damages, injunctive or declaratory relief, and any other relief the court deems proper.

23 62. Plaintiff and Class members are “consumer[s]” as defined by Civ. Code
24 § 1798.140(g) because they are “natural person[s] who [are] California resident[s], as defined in
25 Section 17014 of Title 18 of the California Code of Regulations, as that section read on September
26 1, 2017.”

27
28 ²⁷ California Consumer Privacy Act (CCPA) Compliance, <https://buyergenomics.com/ccpa-compliance/>.

63. Defendant is a “business” as defined by Civ. Code § 1798.140(c) because Defendant:
- a) is a “sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners”;
 - b) “collects consumers’ personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information”;
 - c) does business in and is headquartered in California; and
 - d) has annual gross revenues in excess of \$25 million; annually buys, receives for the business’ commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers’ personal information.

64. The PII accessed and taken by unauthorized persons in the Data Breach is “personal information” as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff’s and other Class members’ unencrypted names, addresses, loan account numbers, and Social Security numbers, among other personal information.

65. Plaintiff’s PII was subject to unauthorized access and exfiltration, theft, or disclosure because his PII, including name, address, loan account number, and Social Security number, at minimum, wrongfully accessed, viewed, and/or taken by unauthorized persons in the Data Breach.

66. The Data Breach occurred as a result of Defendant’s failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff’s and Class members’ PII. Defendant failed to implement reasonable security procedures to prevent an attack on its servers by hackers and to prevent unauthorized access of Plaintiff’s and Class members’ PII as a result of the Data Breach.

67. On or about April 13, 2022, Plaintiff provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). *See* Exhibit A. If Defendant does

1 not cure the violation within 30 days, Plaintiff will amend their complaint to pursue statutory
2 damages as permitted by Civil Code § 1798.150(a)(1)(A).

3 68. As a result of Defendant's failure to implement and maintain reasonable security
4 procedures and practices that resulted in the Data Breach, Plaintiff, on behalf of himself
5 individually and the Class, seeks actual damages, equitable relief, including public injunctive relief,
6 and declaratory relief, and any other relief as deemed appropriate by the Court.

7 **SECOND CAUSE OF ACTION**

8 **Violation of the California Unfair Competition Law ("UCL")**

9 **Cal. Bus. & Prof. Code §§ 17200, *et seq.***

10 69. Plaintiff re-alleges and incorporates by reference all proceeding paragraphs as if fully
11 set forth herein.

12 70. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice
13 and any false or misleading advertising, as those terms are defined by the UCL and relevant case
14 law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary
15 care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair,
16 and fraudulent practices within the meaning, and in violation of, the UCL.

17 71. In the course of conducting its business, Defendant committed "unlawful" business
18 practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee,
19 manage, monitor and audit appropriate data security processes, controls, policies, procedures,
20 protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class
21 members' PII, and by violating the statutory and common law alleged herein, including, *inter alia*,
22 California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100, *et seq.*) and Article I,
23 Section 1 of the California Constitution (California's constitutional right to privacy) and Civil Code
24 § 1798.81.5. Plaintiff and Class members reserve the right to allege other violations of law by
25 Defendant constituting other unlawful business acts or practices. Defendant's above-described
26 wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this
27 date.



72. Defendant also violated the UCL by failing to timely notify Plaintiff and Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiff and Class members had been notified in an appropriate fashion, they could have taken precautions to better safeguard and protect their PII and identities.

73. Defendant’s above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute “unfair” business acts and practices in violation of the UCL in that Defendant’s wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous. Defendant’s practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant’s wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant’s legitimate business interests other than engaging in the above-described wrongful conduct.

74. The UCL also prohibits any “fraudulent business act or practice.” Defendant’s above-described claims, nondisclosures and misleading statements were false, misleading, and likely to deceive the consuming public in violation of the UCL.

75. As a direct and proximate result of Defendant’s above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the UCL, Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) statutory damages under the CCPA, (v) deprivation of the value of their PII for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

76. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of himself, the Class members, and the general public, also seeks restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify its corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

THIRD CAUSE OF ACTION

Breach of Contract

77. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

78. Plaintiff and Class members entered into express contracts with Defendant that included Defendant's promise to protect nonpublic personal information given to Defendant or that Defendant gathered on its own, from unauthorized disclosure.

79. Plaintiff and Class members performed their obligations under the contracts when they provided their PII to Defendant in relation to their payment for Defendant's products and services.

80. Defendant breached its contractual obligation to protect the nonpublic personal information Defendant gathered when the information was exposed as part of the Data Breach.

81. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself individually as well as all members of the Class respectfully requests that (i) this action be certified as a class action, (ii) Plaintiff each be designated a representative of the Class, (iii) Plaintiff's counsel be appointed as counsel for the

Class. Plaintiff, on behalf of himself and members of the Class further request that upon final trial or hearing, judgment be awarded against Defendant for:

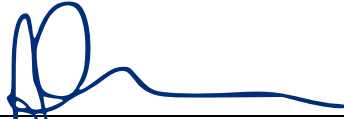
- (i) actual and punitive damages to be determined by the trier of fact;
- (ii) equitable relief, including restitution;
- (iii) pre- and post-judgment interest at the highest legal rates applicable;
- (iv) appropriate injunctive relief;
- (v) attorneys' fees and litigation expenses under Code of Civil Procedure § 1021.5 and other applicable law;
- (vi) costs of suit; and
- (vii) such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial on all issues so triable.

Dated: April 13, 2022

KAZEROUNI LAW GROUP, APC

By: 

ABBAS KAZEROUNIAN, ESQ.
MONA AMINI, ESQ.

Attorneys for Plaintiff

Exhibit “10”



Joseph M. Lyon
jlyon@thelyonfirm.com

June 6, 2022

VIA CERTIFIED MAIL

Corporation Service Company Which Will Do
Business in California as CSC-Lawyers Incorporating Service
2710 Gateway Oaks Drive, Suite 150N
Sacramento, CA 95833-3505

RE: Pingora Loan Servicing, LLC Data Breach – Notice

Dear Pingora Loan Servicing, LLC,

Please take notice my law firm represents Norma Grossman and that this letter is intended to constitute notice under the California Consumer Privacy Act (“CCPA”), California Civil Code section 1798.100, et seq. Per Civil Code Section 1798.150(b), we are hereby notifying Pingora Loan Servicing, LLC (“Pingora”) of the violation of the CCPA, including Section 1798.81.5(b) and Section 1798.150(a)(1), and of our demand that, to the extent you can cure these violations, you cure such violation within thirty (30) calendar days from your receipt of this letter.

Plaintiff Norma Grossman is a resident of California whose personal identifying information (“PII”), including name, address, loan number, and Social Security number as well as potentially any information provided in connection with a loan application, loan modification, or other items related to loan servicing was accessed as a result of an unauthorized individual accessing certain of Pingora’s systems. Plaintiff Norma Grossman received a notice from Pingora informing her that the PII she provided to Pingora was no longer secure.

Please be advised that the failure to prevent Norma Grossman’s and other California residents’ nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure, is a result of Pingora’s failure to meet its duty to implement and maintain reasonable security procedures and practices, which is a violation of Civil Code §§ 1798.81.5 and 1798.150. These failures include the lack of adequate encryption and non-redaction to sufficiently maintain California residents’ PII and to protect this PII from being accessed by third parties without authorization.

Plaintiff Norma Grossman, on behalf of herself and other similarly situated Californians, requests that Pingora immediately cure the CCPA violation which exposed Plaintiff’s and other California consumers’ nonredacted and nonencrypted PII, to the extent there is any possible cure. Please be advised that your failure to comply with this request within thirty (30) calendar days may subject you to statutory damages on an individual and/or class-wide basis.

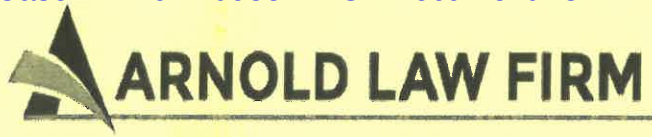
Very truly yours,

THE LYON FIRM

/s/ Joseph M. Lyon

Joseph M. Lyon, Esq.

Exhibit “11”



865 Howe Avenue, Sacramento, CA 95825
7B Corporate Center Court, Greensboro, NC 27408
P: 916-777-7777 | F: 916-924-1829 | justice4you.com

CLAYEO C. ARNOLD
ANTHONY M. ONTIVEROS
JOHN T. STRALEN*
*The Board-Certified Civil
Trial Advocate by the
National Board of Trial
Advocacy

JOSHUA H. WATSON
M. ANDERSON BERRY
ANDREW G. MINNEY
LIYA WALLACE
GREGORY HAROUTUNIAN
JEFFREY J.A. HINRICHS
MICHAEL WELLS
GINA M. BOWDEN**
**Of Counsel

PERSONAL INJURY
WRONGFUL DEATH
EMPLOYMENT LAW
PRODUCT LIABILITY
CLASS ACTION
QUI TAM
DATA BREACH

October 31, 2022

VIA CERTIFIED MAIL

9849 0090 0027 6476 4676 57

Community Loan Servicing, LLC
c/o Legal Department
4425 Ponce De Leon Boulevard, 4th Floor
Coral Gables, FL 33146

VIA CERTIFIED MAIL

9849 0090 0027 6476 4676 71

Bayview Asset Management, LLC
c/o Legal Department
4425 Ponce De Leon Boulevard, 5th Floor
Coral Gables, FL 33146

VIA CERTIFIED MAIL

9849 0090 0027 6476 4676 64

Community Loan Servicing, LLC
c/o Corporation Service Company
Registered Agent
1201 Hays Street
Tallahassee, FL 33146

VIA CERTIFIED MAIL

9849 0090 0027 6476 4676 68

Bayview Asset Management, LLC
c/o Brian E. Bombstein, Esq.
Registered Agent
4425 Ponce De Leon Boulevard, 5th Floor
Coral Gables, FL 33146

RE: Statutory 30-Day Notice of Claim – Cal. Civil Code 1798.100, et seq.

This letter constitutes notice under the California Consumer Privacy Act (“CCPA”), California Civil Code section 1798.100, *et seq.* Pursuant to Civil Code section 1798.150(b), we are hereby notifying Community Loan Servicing, LLC (“Pingora”) and Bayview Asset Management, LLC (“Bayview”) and collectively with Community “Defendants”) that it has violated the CCPA, and we demand that, to the extent any cure exists, Defendants “actually cure[]” such violation within thirty (30) calendar days from the date of this letter.

Our client, Linda Kim, a resident of California, received a Notice of Data Breach from Community on or about October 17, 2022, stating that her personally identifiable information (“PII”) was accessed and no longer secure. The PII exposed includes, at least, name, address, loan number, and Social Security number. *See* CCPA § 1798.81.5(d)(1).

Please be advised that the failure to prevent Linda Kim’s and other California residents’ nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure, is a result of Defendants’ failure to meet their duty to implement and maintain reasonable security procedures and practices, which is a violation of Civil Code §§ 1798.81.5 and 1798.150. These

Community Loan Servicing, LLC
Bayview Asset Management, LLC
October 31, 2022
Page 2

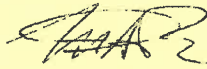
failures include the lack of adequate encryption to sufficiently maintain California residents' PII and to protect this PII from being accessed by third parties without authorization.

To the extent there is any possible cure, we request that Defendants cure this violation which exposed Linda Kim's PII and provide an express written statement that the violations have been "actually cured" and that no further violations will occur. A cure, if possible, would require Defendants to, for example, recover all of the stolen PII and eliminate any future risk that Linda Kim's stolen PII is accessed.

A failure to comply with this request within thirty (30) calendar days will subject Defendants to statutory damages on an individual and/or class-wide basis.

Thank you for your time and cooperation.

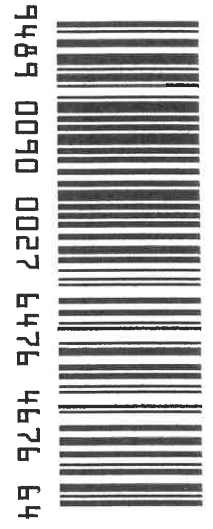
Very truly yours,



M. Anderson Berry, Esq.
aberry@justice4you.com
(916) 239-4778

MAB:lm


ARNOLD LAW FIRM
865 Howe Avenue, Sacramento, CA 95825



Label 890-PB, Oct. 2015
Pitney Bowes

FIRST-CLASS




US POSTAGE
ZIP 95825
02 7H
0006025330
\$ 007.82⁰
OCT 31 2022

Bayview Asset Management, LLC
c/o Brian E. Bombstein, Esq.
Registered Agent
1201 Ponce De Leon Boulevard, 5th Floor
Coral Gables, FL 33146


ARNOLD LAW FII
865 Howe Avenue, Sacramento, CA 95825



Label 890-PB, Oct. 2015
Pitney Bowes

FIRST-CLASS



US POSTAGE 
ZIP 95825
02 7H
0006025330
\$ 007.82⁰
OCT 31 2022

Bayview Asset Management, LLC
c/o Legal Department
4425 Ponce De Leon Boulevard, 5th Floor
Coral Gables, FL 33146



865 Howe Avenue, Sacramento, CA 95825

9489 0090 0027 6476 4676 71



Label 890-PB, Oct. 201
Pitney Bowes

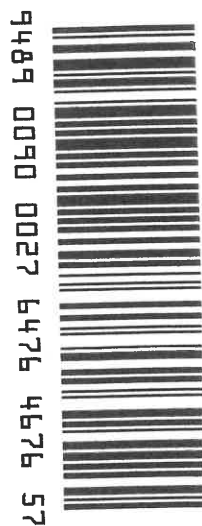
FIRST-CLASS



US POSTAGE  PITNEY BOWES
ZIP 95825
02 7H
0006025330 OCT 31 2022
\$ 007.820

Community Loan Servicing, LLC
c/o Corporation Service Company
Registered Agent
1201 Hays Street
Tallahassee, FL 33146


ARNOLD LAW FIRM
865 Howe Avenue, Sacramento, CA 95825



Label 890-PB, Oct. 2015
Pitney Bowes

FIRST-CLASS



US POSTAGE

ZIP 95825
02 7H
0006025330
OCT 31 2022
\$ 007.82

Community Loan Servicing, LLC
c/o Legal Department
4425 Ponce De Leon Boulevard, 4th Floor
Coral Gables, FL 33146

Exhibit “12”



Statement of Work

This Statement of Work is valid when signed before December 31, 2021.

This Statement of Work ("SOW") is made and entered into as of the later of the signature dates below ("SOW Effective Date"), by and between Mandiant and Baker & Hostetler LLP ("Counsel") for the benefit of Bayview Asset Management, LLC ("Customer"). This SOW is governed by the Master Services Agreement (the "Agreement") dated October 4, 2019 between Customer and Mandiant. Capitalized terms used in this SOW will have the meanings given to them in the Agreement. Services performed outside the Americas will be performed and invoiced by Mandiant Ireland Limited, regardless of which Mandiant entity is party to this SOW, and in such cases Mandiant Ireland Limited will be deemed "Mandiant" as set forth in this SOW. Services performed within the Americas will be performed and invoiced by Mandiant, Inc., regardless of which Mandiant entity is party to this SOW, and in such cases Mandiant, Inc. will be deemed "Mandiant" as set forth in this SOW.

1. Description of Services

Mandiant agrees to provide services ("Services") as set forth below, as directed by Counsel for the benefit of Customer.

1.1. Incident Response

The objective of this professional services engagement is to assist Counsel in providing legal advice to Customer with responding to a suspected security incident and in anticipation of litigation that may arise from the incident. The activities to be performed may include but are not limited to the following:

- Computer security incident response support.
- Digital forensics, log analysis, and malware analysis support.
- Incident remediation assistance.
- Deployment support for Mandiant's incident response technologies.
- Regular status reporting and project management-related activities.
- Reporting and/or presentations associated with findings and recommendations.

Customer acknowledges that Mandiant may use other tools, including cloud-based technologies and email monitoring systems, in the course of performing Services, and agrees that Mandiant may use all such tools in its discretion.

All parties acknowledge that Mandiant can leverage the technology stacks currently installed in Customer's environment during the course of the engagement, if any ("Customer-Owned Technology"). If Mandiant determines that the Customer-Owned Technology cannot adequately support the performance of the Services, additional technology stacks may be deployed in the Customer's environment and, in such case, will be invoiced as set forth in Section 5.

2. Deliverables

2.1. Incident Response Deliverables

The following Deliverables will be produced for these Services during the course of this engagement:

- Regular Status Reporting: Mandiant will provide regular status reporting that summarizes activities completed, significant findings, issues requiring attention and plans for the next reporting period.
- Incident Response Report: If requested by Counsel, Mandiant will provide a written summary of the incident response results. This typically includes a summary of activity, detailed activity description, supporting analysis, and remediation recommendations.
- Executive Briefing: If requested by Counsel, Mandiant will provide an executive brief that summarizes the incident response, including the investigation and remedial activities.

Any other reports (including intelligence reports), presentations, materials or other written information provided by Mandiant as a result of the Services are Mandiant Materials and will not be considered "Deliverables" as defined in the Agreement.



Statement of Work

3. Schedule and Staffing

The scheduling of Services under this SOW will be as mutually agreed to by all parties. The Services under this SOW will be provided within the twelve (12) month period from the SOW Effective Date.

4. Services Fees

All work will be performed on a time and materials basis at the rate of [REDACTED] for consulting Services performed. In consideration for the Services to be performed by Mandiant, Customer agrees to pay for actual time spent. Travel time related to Services performed onsite will be invoiced [REDACTED]. Invoices will be issued monthly. If Customer is working with an insurer, Customer will be responsible for payment of all fees and expenses, regardless of whether the insurer provides coverage or reimbursement for all or part of the fees and expenses described herein.

Customer will pay all invoices as set forth in the Agreement. All fees are non-cancelable and non-refundable. Customer agrees that this SOW represents the complete, final, and exclusive terms and conditions governing the Services. As such, Mandiant may invoice Customer in advance, unless otherwise stated in this SOW, without the requirement that Customer provide a subsequent purchase order. Any such subsequently issued purchase order shall be for administrative purposes only.

5. Technology Fees

Mandiant will determine the technology that is required to support the Services under this SOW. Customer agrees to pay technology fees from the date of delivery at the price per unit quoted in the table below. These fees will be invoiced monthly and charged to the nearest whole month; they are not pro-rated.

Unit Description	Price per Unit
Endpoint Incident Response Technology	
Cloud up to 100 nodes	
Cloud up to 1,000 nodes	
Cloud up to 10,000 nodes	
Hardware appliance, up to 10,000 nodes	
Supplemental up to 10,000 nodes	
Off-Hours Alert Monitoring	
Endpoint count: up to 500 nodes	
Endpoint count: up to 1,000 nodes	
Endpoint count: up to 5,000 nodes	
Endpoint count: up to 10,000 nodes	
Endpoint count: up to 20,000 nodes	
Endpoint count: up to 50,000 nodes	
Over 50,000 nodes	
Network Incident Response Technology	



Statement of Work

Unit Description	Price per Unit
1Gb appliance (Maximum throughput 950Mbps)	
10Gb appliance (Maximum throughput 4.5Gbps)	
10Gb XL appliance (Maximum throughput 9Gbps)	
Cloud-Based Log Analysis Technology	
Instance up to 5,000 events per second, 10TB storage, 30 day retention	
Instance up to 10,000 events per second, 20TB storage, 30 day retention	
Email Incident Response Technology – Cloud with AV/AS	
100-499 inboxes	
500-999 inboxes	
1000-1999 inboxes	
2000-4999 inboxes	
5000-9999 inboxes	
>10,000 inboxes	
Managed Defense Continuous Vigilance	
Node count: up to 499 nodes	
Node count: up to 999 nodes	
Node count: up to 4,999 nodes	
Node count: up to 9,999 nodes	
Node count: up to 19,999 nodes	
Node count: up to 49,999 nodes	
Node count: up to 75,999 nodes	
Node count: up to 99,999 nodes	
Node count: up to 999,999 nodes	
Evidence Storage	
Storage of each physical evidence item	
Other	
Domestic shipping and handling of hardware	
International shipping and handling of hardware	
Custom Dark Web Search – No Report	

In addition to the technology listed in the table above, Mandiant may require the use of other tools to facilitate the investigation. Mandiant will request written (emailed) authorization from Customer for any charges related to the use of technologies not detailed in the above table.



Statement of Work

6. Fee Estimates

Itemized fee estimates are provided in the table below.

Description	Estimated Quantity	Estimated Cost	
Professional Services			
Incident response activities including, but not limited to: - Endpoint sweeping and forensic analysis - Network monitoring and analysis - Log analysis - Malware analysis and reverse engineering - Threat analysis and intelligence - Status reporting	450 hours		
Incident containment planning and support	50		
Reporting and out-brief including, but not limited to: - Incident Investigation Report - Incident Remediation Report	TBD		
Technology			
Endpoint Incident Response Technology Cloud up to 1,000 nodes	2 months		
Off-Hours Alert Monitoring Endpoint count: up to 1,00 nodes	2 months		
Other			
Custom Dark Web Search – No Report	1		
Total Estimated Fees			

7. Expenses

Customer shall reimburse for the following expense categories that are directly attributable to work performed under this SOW:

- Travel and living expenses.
- Mileage in company or personal vehicles at the rate approved by the U.S. Internal Revenue Service.
- Computer storage media.
- Postage and courier services.
- Printing, reproduction and binding.
- Any other expenses resulting from the work performed under this SOW.



Statement of Work

Upon request Mandiant will provide electronic copies of expense receipts for all expense related items greater than \$25. Invoices for expenses will be issued on a monthly basis.

8. Assumptions

1. All work activities will be performed without day and time restrictions.
2. If any factor outside Mandiant's control, including those caused by Customer or Customer requirements (such as requirements to refrain from operating technology during specific times), causes delays in implementing technology needed for Mandiant to perform the Services or cause Services to take longer than expected, then notwithstanding any fixed fees, Customer will be invoiced for technology fees for the period of any such delays.
3. Estimated professional fees do not include any hardware, software, licensing, maintenance, or support costs of any Mandiant or other third-party product or service suggested by Mandiant as we conduct the activities outlined within this SOW.
4. Mandiant will provide Deliverables to Customer throughout this engagement. Draft Deliverables are considered final upon confirmation from Customer (written or oral) or ten business days after their submission date from Mandiant to Customer, whichever is earlier.
5. When Mandiant's personnel are performing Services on site at Customer's premises, Customer will allocate appropriate working space and physical access for all Mandiant assigned personnel.
6. Customer represents that all information provided is true and accurate and that Customer owns or is authorized to represent the owners of the systems, facilities, and/or devices described in connection with the services. Customer represents that it has obtained all permissions necessary for Mandiant to perform the services described herein. Customer will hold Mandiant harmless against any claims, disputes, or issues arising or related to foregoing representations.
7. Customer will make available key individuals that can best help plan operations around security event monitoring, analysis, threat intelligence, and incident response.
8. Any changes to the scope of Services or this SOW must be mutually agreed upon in writing by all parties.

9. Contact Information

Customer will provide Mandiant with points of contact information in the following table:

Business Line Contact	
Name:	
Title:	
Email:	
Phone:	
Street:	
City:	
State:	
Zip:	
Payables Contact	
Name:	
Title:	
Email:	



Statement of Work

Phone:	
Street:	
City:	
State:	
Zip:	

Claim Manager Contact	
Name	Matthew Basilotto, Esq.
Email	matthew.basilotto@chubb.com
Claim #	KY21K3025077

10. Signatures

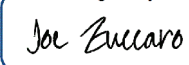
Mandiant and Customer have executed this Statement of Work as of the SOW Effective Date.

[Signature Page Follows]



Statement of Work

Mandiant, Inc.

DocuSigned by:

87A99893983E4B7...
Joe Zuccaro

Name
VP Commercial Legal Americas

Title
12/12/2021 | 10:17 AM PST

Date

Bayview Asset Management, LLC

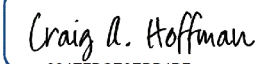
DocuSigned by:

77E51620648D4B9...
Signature
Brian Bomstein

Name
Senior Vice President

Title
12/11/2021 | 12:37 PM PST

Date

Baker DocuSigned by:

834E7BCE8EBB4D7...
Signature
Craig A. Hoffman

Name
Partner

Title
12/11/2021 | 12:35 PM PST

Date

Exhibit “13”
To Be Filed Under Seal

Exhibit “14”
To Be Filed Under Seal