**IN THE UNITED STATES DISTRICT COURT**
**DISTRICT OF MASSACHUSETTS**

| | |
|---|---|
| **ROBERTO CERDA, individually and on behalf of all others similarly situated,**<br><br>**Plaintiff,**<br><br>vs.<br><br>**ALVARIA, INC., CARRINGTON MORTGAGE SERVICES, LLC,**<br><br>**Defendant.** | Case No.<br><br>**CLASS ACTION COMPLAINT**<br><br>**DEMAND FOR JURY TRIAL** |

Plaintiff ROBERTO CERDA ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Consolidated Class Action Complaint against ALVARIA, INC. ("Alvaria") and CARRINGTON MORTGAGE SERVICES, LLC ("Carrington") (collectively referred to as the "Defendants") and alleges, upon personal knowledge as to their own actions and their counsel's investigations, and upon information and belief as to all other matters, as follows:

## I. INTRODUCTION

1. This action stems from Defendants' failure to secure the sensitive personal information of Carrington's current and former customers and other consumers for whom Alvaria performed services.

2. Defendant Alvaria is a business software company based in Westford, Massachusetts and was recently formed through the merger of Aspect Software and Noble Systems

in or around May of 2021.[1] Alvaria employs more than 2,000 people and generates approximately $423 million in annual revenue.[2]

3. Defendant Carrington is a mortgage services provider based in Anaheim, California that offers a variety of mortgage products in all 50 states.[3] Defendant Carrington employs more than 2,716 people and generates approximately $1.2 billion in annual revenue.[4]

4. Defendant Alvaria provides software services to its business clients and obtains certain personally identifying information due to the services it provides. Specifically, Defendant Alvaria obtains personally identifying information from the customers of its business clients and stores this sensitive information for its own benefit.

5. Defendant Carrington provides mortgage services to its customers and obtains certain personally identifying information due to the services it provides. Specifically, Defendant Carrington obtains personally identifying information from its customers and stores this sensitive information for its own benefit.

6. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard sensitive personally identifiable information provided by, and belonging to, their customers and the customers of their clients, including, without limitation, names, mailing addresses, telephone numbers, loan numbers, current loan balances, and the last four digits of Social Security numbers.

---

[1] *See* https://www.alvaria.com/company/about-alvaria (last visited May 12, 2023).
[2] *See* https://www.jdsupra.com/legalnews/alvaria-inc-files-data-breach-notice-on-6972963/ (last visited May 12, 2023).
[3] *Id.*
[4] *Id.*

7. On or around March 9, 2023, Alvaria was the victim of a sophisticated ransomware attack on a portion of its "customer environment" that maintained "some of [its] customers' workforce management and/or outbound dialer data." (the "Data Breach").[5] This ransomware attack involved personal information that came into Alvaria's possession through Carrington who provided Alvaria access to their customers' personal information.[6] [7]

8. This is the second security incident that Alvaria has suffered in the last four months. In November of 2022, Alvaria suffered a cybersecurity attack by the Hive Ransomware group. This incident impacted nearly 5,000 customers.[8]

9. Upon discovery of the Data Breach, Alvaria initiated an investigation of the incident with the assistance of forensic experts and determined that "on March 9, 2023, the unauthorized actor obtained access to and procured some data associated with Carrington Mortgage Services, LLC, which may have contained [] personal information."[9] Carrington is a large mortgage service provider that "services loans in all 50 states and Puerto Rico and is licensed to lend in 48 states."[10] As such, individuals across every state may have been affected Defendants' Data Breach.

10. On or around April 26, 2023, Defendants began notifying Plaintiff and Class Members of the Data Breach.

---

[5] *See* Ex. 1 (Letter to Plaintiff entitled "Notice of Data Incident" dated April 26, 2023.)
[6] *See* https://www.iowaattorneygeneral.gov/media/cms/4262023_Carrington_Mortgage_Service_FFBA0CD237FA1.pdf (last visited May 12, 2023).
[7] *Id.*
[8] Tech vendor names Carrington in data breach notice, NEXT, May 3, 2023, https://nextmortgagenews.com/news/tech-vendor-names-carrington-in-data-breachnotice/ (last visited May 12, 2023).
[9] *Id*.
[10] *See* https://www.carringtonmortgage.com/our-mission (last visited May 12, 2023).

11. In the notices sent to Plaintiff and Class Members, Defendants recognized that each Class Member is now subject to the present and continuing risk of identity theft and fraud, by offering Plaintiff and Class Members limited identity theft protection from Experian.[11] Defendants also direct Plaintiff and Class Members "to remain vigilant against the potential for identity theft and fraud and to monitor [their] accounts and credit reports for any suspicious activity."[12] The offered services, however, fall well short of what is needed to protect Plaintiff and Class Members from the lifelong implications of having their most private PII accessed, acquired, exfiltrated, and/or published on the internet. As one element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide to Plaintiff and Class Members enhanced identity theft protection services for their respective lifetimes.

12. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties to these individuals to safeguard and protect the PII from unauthorized access. Defendants admit that the unencrypted PII accessed and exfiltrated includes highly sensitive information, such as names, mailing addresses, telephone numbers, loan numbers, current loan balances, and the last four digits of Social Security numbers.[13]

13. The exposed PII of Plaintiff and Class Members can be, and in certain cases has 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 personal information captured through means such as data breaches or hacks)."[14]

---

[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited May 12, 2023).

14. Plaintiff is informed and believes that his information has already been placed onto the dark web. Hackers can now access and/or offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members face an ongoing and lifetime risk of identity theft, which is heightened by the loss of their Social Security numbers.

15. This PII was compromised due to Defendants' negligent and/or careless acts and omissions and their failure to protect PII of Plaintiff and Class Members.

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

17. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of their inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities. Defendants' conduct amounts to at least negligence and violates federal and state statutes designed to prevent or mitigate this very harm.

18. Plaintiff and Class Members 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 emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) 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; (g) damages to and diminution in value of their personal data entrusted to Defendants on the mutual understanding that Defendants would safeguard their PII against theft and not allow access to and misuse of their personal data by others; and (h) the continued risk to their PII, which remains in the possession of Defendants, and which is subject to further injurious breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII. Plaintiff and Class Members, at the very least, are entitled to damages and injunctive relief tailored to address the vulnerabilities exploited in the breach, and designed to protect Plaintiff's and Class Members' PII, as well as an order from the Court directing the destruction and deletion of all PII for which Defendants cannot demonstrate a reasonable and legitimate purpose for continuing to maintain possession of such PII.

19. Defendants understand the need to protect the privacy of their business clients' customers and use security measures to protect their clients' customers' information from unauthorized disclosure.[15] [16] As sophisticated financial entities who maintain private and sensitive consumer information, Defendants further understood the importance of safeguarding PII. Yet Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff 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 protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through access to and exfiltration

[15] *See* https://www.alvaria.com/legal/privacy-policy (last visited May 12, 2023).
[16] *See* https://www.carringtonmortgage.com/legal/privacy-policy (last visited May 12, 2023).

by an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

20. Plaintiff by this action seeks compensatory damages together with injunctive relief to remediate Defendants' failures to secure his and the other Class Members' PII, and to provide damages, for among other things, for Plaintiff and Class Members to secure identity theft insurance, and credit repair services for Class Members' respective lifetimes to protect each Class of Data Breach victims from identity theft and fraud.

## II. PARTIES

***Plaintiff Roberto Cerda***

21. Plaintiff Roberto Cerda is a resident and citizen of the State of Florida.

***Defendant Alvaria, Inc.***

22. Defendant Alvaria, Inc. is a business software company organized under the laws of Delaware and headquartered at 5 Technology Park Drive, Westford, Massachusetts 01886.

23. All of Plaintiff's claims stated against Defendant Alvaria herein are also asserted against and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

***Defendant Carrington Mortgage Services, LLC***

24. Defendant Carrington Mortgage Services, LLC is a mortgage service provider organized under the laws of Delaware and headquartered at 1600 S. Douglass Rd., Suites 200-A & 110, Anaheim, CA 92806.

25. All of Plaintiff's claims stated against Defendant Carrington herein are also asserted against any of its owners, predecessors, subsidiaries, agents and/or assigns.

## III. JURISDICTION AND VENUE

26. 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 $5,000,000.00 exclusive of interest and costs. Moreover, the minimal diversity requirement is met as Plaintiff, Class Members, and Defendants are citizens of different states.

27. The Court has personal jurisdiction over Defendant Alvaria because, personally or through their agents, Defendant Alvaria operated, conducted, engaged in, or carried on a business or business venture in Massachusetts; had offices in Massachusetts; committed tortious acts in Massachusetts; and/or breached a contract in Massachusetts by failing to perform acts required by the contract to be performed in Massachusetts. Defendant Alvaria is also headquartered in Westford, Massachusetts.

28. The Court has personal jurisdiction over Defendant Carrington because, personally or through their agents, Defendant Carrington operated, conducted, engaged in, or carried on a business or business venture in Massachusetts; had offices in Massachusetts; committed tortious acts in Massachusetts; and/or breached a contract in Massachusetts by failing to perform acts required by the contract to be performed in Massachusetts. Defendant Carrington is also registered to do business in Massachusetts, has a registered agent for service of process in Massachusetts, has a Massachusetts Debt Collector License, [17] transacts business in Massachusetts, and/or contracts to supply services or things in Massachusetts, as provided in M.G.L., c. 223A, § 3(a) and (b).

[17] https://www.carringtonmortgage.com/legal/state-licensing (last visited May 12, 2023).

29. 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 conduct substantial business in this district and reside in this district. Further, on information and belief, decisions regarding the management of the information security of Plaintiff's and Class Members' PII were made by Defendants within this district. Moreover, it is believed that Defendants maintain Plaintiff's and Class Members PII in the district, and the harm caused to Plaintiff and Class Members emanated from this district.

## IV. FACTUAL ALLEGATIONS

***Background***

30. Defendant Alvaria is a large business software company that specializes in "delivering optimized customer experience and workforce engagement software and cloud services technology solutions."[18]

31. Defendant Carrington is a is a large mortgage service provider that "services loans in all 50 states and Puerto Rico and is licensed to lend in 48 states."[19]

32. Plaintiff and Class Members are individuals who received or applied for services from Defendant Carrington and thereby Defendant Alvaria. Thus, Plaintiff and Class members were required to entrust some of their most sensitive and confidential information to the care of Defendants, including, without limitation: names, mailing addresses, telephone numbers, loan numbers, current loan balances, and the last four digits of Social Security numbers. Much of the information Plaintiff and Class Members entrusted to Defendants is static, does not change, and can be used to commit myriad financial crimes.

---

[18] *See* https://www.alvaria.com/company/about-alvaria (last visited May 12, 2023).
[19] *See* Footnote No. 9.

33. In providing services to their clients, Plaintiff, and Class Members, Defendants generated and retained additional sensitive personal information about Plaintiff and Class Members.

34. Sophisticated companies like Defendants are aware of the different types of threat actors acting across the Internet and the type of criminal cybersecurity acts they employ for profit. Accordingly, it is imperative that Defendants guard against those criminal exploits.

35. Plaintiff and Class Members as current and former customers of Defendants and Defendants' business clients 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 information.

36. Defendants had a duty to adopt reasonable measures to protect Plaintiff's 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 were aware of the consequences to Plaintiff and Class Members if they failed to adequately protect that information. Defendants breached their duty to Plaintiff and Class Members and allowed an attacker access to their systems without detection.

37. Defendants knew that the PII they maintained was a target of data thieves and that they had a duty to protect Plaintiff's and Class Members' PII from unauthorized access. For example, Defendants post Privacy Policies on their websites. The Privacy Policies promise consumers that Defendant, "maintain[s] appropriate physical, electronic, procedural, technical and organizational measures to help safeguard personal information from loss, theft, misuse, unauthorized access, disclosure, alteration and destruction"[20] and that their "hosting services

[20] *See* Footnote Nos. 14 & 15.

maintain their systems in accordance with reasonable industry standards to reasonably secure the information of its customers."[21] These Privacy Policies also acknowledge that Defendants collect consumer data directly from business clients and consumers and via their affiliates.

38. Moreover, Defendants are sophisticated companies that knew or should have known that PII, including Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

39. Defendants knew or should have known that these attacks were common and foreseeable. In 2022, there were 1,802 data breaches, nearly eclipsing 2021's record wherein 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[22] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[23]

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

---

[21] *Id.*

[22] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6 (last visited May 12, 2023).

[23] See *Data Breaches Hit Lots More People in 2022* (Jan. 25, 2023) https://www.cnet.com/tech/services-and-software/data-breaches-hit-lots-more-people-in-2022/ (last visited May 12, 2023).

41. Additionally, Defendants have even further awareness of such attacks because only four months prior in November 2022, Defendant Alvaria suffered a similar data breach at the hands of the Hive Ransomware group.[24]

42. Indeed, cyberattacks have become so notorious that the FBI and U.S. 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.

43. Despite the prevalence of public announcements of data breach and data security compromises, and Defendant Alvaria's own recent data breach in November 2022, Defendants failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

***The Data Breach***

44. On or about March 9, 2023, an intruder gained unauthorized access to Defendants' "customer environment."[25] Defendants discovered the intrusion around that same time.

45. Defendants reported the breach to the Massachusetts Office of Consumer Affairs and Business Regulation on April 26, 2023.[26]

46. Beginning on or around April 26, 2023, Defendants began sending a letter entitled "Notice of Data Incident" to affected individuals.[27]

47. This letter to Plaintiff and Class Members stated the following:

> Alvaria, Inc. ("Alvaria") is a workforce management and call center technology solution company. We write to inform you about a recent incident experienced by Alvaria that may have involved some of your personal information, which came into our possession due to the

[24] *See* Footnote No. 7.
[25] *See* Ex. 1
[26] *See* https://www.mass.gov/doc/data-breach-report-2023/download (last visited May 12, 2023).
[27] *See* Ex. 1.

> services we provide Carrington Mortgage Services, LLC. We are providing you with information about the incident and steps you can take to protect yourself, should you feel it necessary to do so.
>
> **What Happened?**
>
> On March 9, 2023, Alvaria was the victim of a sophisticated ransomware attack on a portion of our customer environment that maintained some of our customers' workforce management and/or outbound dialer data. Upon discovery, we immediately secured our networks, safely restored our systems and operations via viable backups, and initiated an investigation of the incident with the assistance of forensic experts. Our investigation determined that, on March 9, 2023, the unauthorized actor obtained access to and procured some data associated with Carrington Mortgage Services, LLC, which may have contained your personal information. Presently, we have no evidence of actual or attempted misuse of your personal information.
>
> **What Information Was Involved?**
>
> The impacted files may have contained your personal information, including your name, mailing address, telephone number, loan number, current loan balance, and the last four digits of your Social Security number.
>
> **What We Are Doing.**
>
> Upon discovery of the incident, we immediately secured our networks, implemented measures to further improve the security of our systems, safely restored our systems and operations via viable backups, initiated an investigation of the incident with the assistance of forensic experts, and notified the Federal Bureau of Investigation ("FBI"). We also are notifying you so that you may take further steps to protect your information, should you feel it appropriate to do so. In addition, we are providing you with access to 24 months of credit monitoring and identity restoration services through Experian at no charge to you. You must enroll by July 31, 2023.[28]

48. Defendants admit in the letter that unauthorized third persons accessed and removed from their network systems sensitive information about current and former customers of themselves

[28] *Id.*

and its affiliates including, without limitation: "names, mailing addresses, telephone numbers, loan numbers, current loan balances, and the last four digits of [] Social Security numbers."[29] Much of this sensitive information is static, cannot change, and can be used to commit myriad financial crimes.

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

50. Defendants did not use reasonable security procedures and practices suitable or adequate to protect the sensitive, unencrypted information it was maintaining for consumers, causing the access and/or exfiltration of the PII of the affected individuals.

***Defendants Acquire, Collect and Store Plaintiff's and Class Members' PII.***

51. Defendants acquired, collected, and stored the PII of current and former customers and those of their affiliates.

52. As a condition of receiving services from Defendants, Defendants require that consumers entrust them with highly confidential PII.

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

---

[29] *Id.*

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

***Securing PII and Preventing Breaches***

55. Defendants could have prevented this Data Breach by properly securing and/or encrypting Plaintiff's and Class Members' PII. Additionally, Defendants could have destroyed data, including old data that Defendants had no legal right or responsibility to retain.

56. Defendants' negligence in safeguarding Plaintiff's and Class Members' PII is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data, especially sensitive financial data, and the recent data breach suffered by Defendant Alvaria.

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

58. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[30] 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, [and] employer or taxpayer identification number."[31]

---

[30] 17 C.F.R. § 248.201 (2013).
[31] *Id.*

59. The ramifications of Defendants' failure to keep secure Plaintiff's and Class Members' PII are long lasting and severe. Once Social Security numbers and other PII have been stolen, fraudulent use of that information and damage to victims may continue for years.

***Value of Personal Identifiable Information***

60. PII is very 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.[32] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[33] Criminals also can purchase access to entire sets of information obtained from company data breaches from $900 to $4,500.[34]

61. Social Security numbers are among the most sensitive kinds 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

---

[32] *Your Personal Data Is for Sale on the Dark Web. Here's How Much It Costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed May 12, 2023).

[33] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed May 12, 2023).

[34] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed May 12, 2023).

> never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[35]

62. 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.

63. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[36]

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

65. This data commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally

---

[35] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed May 12, 2023).

[36] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed May 12, 2023).

identifiable information and Social Security numbers are worth more than 10x on the black market."[37]

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

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

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[38]

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

---

[37] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed May 12, 2023).

[38] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last visited May 12, 2023).

70. Plaintiff and Class Members now face a lifetime of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring, and will continue to incur, such damage in addition to any fraudulent use of their PII.

71. 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 harmed by the exposure of the unencrypted data.

72. Although Defendants have offered identity monitoring services for a limited time through Experian, the offered services are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the highly sensitive nature of the PII at issue here.

73. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of their current and former customers.

## V. PLAINTIFF-SPECIFIC ALLEGATIONS

***Plaintiff Roberto Cerda's Experience***

74. Plaintiff Cerda used Carrington Mortgage's services when he took out a mortgage on his home. As a condition to receiving loan services from Carrington, Plaintiff Cerda provided his PII to Carrington which was then entered into Carrington's database and maintained by Carrington.

75. Unbeknownst to Plaintiff Cerda, the PII he entrusted to Carrington was shared with Defendant Alvaria. As such, the PII he entrusted to Carrington, that was then shared with Alvaria, was entered into Alvaria's database and maintained by Alvaria.

76. Plaintiff Cerda greatly values his privacy and PII, especially when receiving loans and other financial services. Prior to the Data Breach, Plaintiff Cerda took reasonable steps to maintain the confidentiality of his PII.

77. Plaintiff Cerda received a letter dated April 26, 2023, from Defendant Alvaria, on behalf of Defendant Carrington, concerning the Data Breach. The letter stated that unauthorized actors gained access to files on Alvaria's network that contained his name, mailing address, telephone number, loan number, current loan balance, and the last four digits of his Social Security number.

78. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Cerda faces, Defendant offered him a two-year subscription to a credit monitoring service.

79. Since learning of the Data Breach, Plaintiff Cerda has spent additional time reviewing his bank statements and credit cards. Since April 2023, he has spent approximately two hours every day reviewing his accounts and credit reports. Plaintiff spent this time at Defendants' direction because in the notice letter Plaintiff received, Defendants directed Plaintiff to spend time mitigating his losses by "monitoring [his] accounts and credit reports for any suspicious activity."

80. Plaintiff Cerda has experienced an increase of other spam calls and text messages after the Data Breach.

81. The Data Breach has caused Plaintiff Cerda to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have not been forthright with information about the Data Breach. Plaintiff has been particularly anxious and worried that his credit may be compromised, including information affecting his mortgage.

///

///

82. Plaintiff Cerda 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.

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

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

85. Plaintiff Cerda 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's and Class Members' Injuries and Damages***

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

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

88. Plaintiff 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 Plaintiff and Class Members.

89. Plaintiff and Class Members are also incurring and may continue incurring out-of-pocket costs for protective measures such as 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.

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

91. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendants and their affiliates was intended to be used by Defendants to fund adequate security of Defendants' computer property and protect Plaintiff's and Class Members' PII. Thus, Plaintiff and Class Members did not get what they paid for.

92. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse. Indeed, Defendants' own notice of data breach provides instructions to Plaintiff and Class Members about all the time that they will need to spend monitoring their own accounts and credit reports.

93. Plaintiff 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 number, medical insurance accounts, bank accounts, payment card statements, and credit reports for unauthorized activity for years to come.

94. Moreover, Plaintiff 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, and/or financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

95. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

96. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at a substantial and present risk of harm.

## VI. CLASS ALLEGATIONS

97. 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), Plaintiff brings this Action on behalf of himself and on behalf of all other persons similarly situated. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> All individuals residing in the United States whose PII was accessed or exfiltrated during the Data Breach announced by Defendants in April of 2023 (the "Class");

98. Excluded from the Class 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.

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

100. Numerosity. Consistent with Fed. R. Civ. P. 23(a)(1), the Class Members are so numerous that their joinder is impracticable. The number and identities of Class Members can be ascertained through Defendants' records.

101. 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 but are not limited to:

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

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

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

d. Whether Defendants had a duty not to use the PII of Plaintiff 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 Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendants failed to promptly notify Plaintiff and Class Members that their PII had been compromised;

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

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

j. Whether Defendants violated state statutes as alleged herein;

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

l. Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

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

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

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

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

105. 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.

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

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

## COUNT I
## NEGLIGENCE
## (On Behalf of Plaintiff and the Class)

108. Plaintiff re-alleges and incorporates paragraphs 1-107 as if fully set forth herein.

109. As a condition of receiving their mortgages or related services from Defendants or their clients, partners or affiliates, Plaintiff and Class Members were obligated to provide and entrust Defendants with certain PII, including their names, mailing addresses, telephone numbers, loan numbers, current loan balances, and the last four digits of Social Security numbers.

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

111. By undertaking the duty to maintain and secure this data, sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard

their systems and networks—and Plaintiff and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from cyber theft.

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

113. Defendants knew or reasonably should have known that their failure to exercise due care in the collecting, storing, and using of consumers' PII involved an unreasonable risk of harm to Plaintiff and Class Members, including harm that foreseeably could occur through the criminal acts of a third party.

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

115. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former business client customers' and direct customers' PII that they were no longer required to retain pursuant to regulations.

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

117. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and Class Members. That special relationship arose because Plaintiff and Class Members entrusted Defendants, their affiliates, and

their business clients with their confidential PII, a mandatory step in receiving services from Defendants. While this special relationship exists independent from any contract, it is recognized by Defendants' Privacy Policies, as well as applicable laws and regulations. Specifically, Defendants actively solicited and gathered PII as part of their businesses and were solely responsible for and in the position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a resulting data breach.

118. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiff and Class Members, to maintain adequate data security.

119. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

120. Defendants also had a common law duty to prevent foreseeable harm to others. Plaintiff and Class Members were the foreseeable and probable victims of Defendants' inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and Class Members, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendants' systems. It was foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

121. Defendants' conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendants' wrongful conduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also

included their decision not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII, including basic encryption techniques available to Defendants.

122. Plaintiff and Class Members had and have no ability to protect their PII that was in, and remains in, Defendants' possession.

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

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

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

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

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

128. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect their, and their business clients', current and former customers', PII in the face of increased risk of theft.

129. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of their, and their business clients', current and former customers' PII.

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

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

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

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

134. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of businesses, such as Defendants, of failing to implement reasonable measures to protect PII. The FTC Act and related authorities form part of the basis of Defendants' duty in this regard.

135. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained

and stored and the foreseeable consequences of the damages that would result to Plaintiff and Class Members.

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

137. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

138. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

139. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's 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 continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect their, and their business clients', current and former customers' PII in their continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair

the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

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

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

143. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff 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 IMPLIED CONTRACT
## (On Behalf of Plaintiff and the Class)

144. Plaintiff re-alleges and incorporates paragraphs 1-107 as if fully set forth herein.

145. Defendants acquired and maintained the PII of Plaintiff and Class Members, including names, mailing addresses, telephone numbers, loan numbers, current loan balances, and the last four digits of Social Security numbers.

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

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

148. Prior to the Data Breach, Defendants each published a Privacy Policy, agreeing to protect and keep private financial information of Plaintiff and Class Members.

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

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

151. In collecting and maintaining the PII of Plaintiff and Class Members and publishing their privacy policies, Defendants entered into contracts with Plaintiff and Class Members requiring Defendants to protect and keep secure the PII of Plaintiff and Class Members.

152. Plaintiff and Class Members fully performed their obligations under the contracts with Defendants.

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

154. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff 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; expenses and/or time spent on credit monitoring and identity theft insurance; additional time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, credit freezes; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

155. As a direct and proximate result of Defendants' breach of contract, Plaintiff and Class Members are at an increased risk of identity theft or fraud.

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

## COUNT III
## BREACH OF FIDUCIARY DUTY
## (On Behalf of Plaintiff and the Class)

157. Plaintiff re-alleges and incorporates paragraphs 1-107 as if fully set forth herein.

158. A relationship existed between Plaintiff and Class Members Class and Defendants in which Plaintiff and Class Members put their trust in Defendants to protect the private information of Plaintiff and Class Members and Defendants accepted that trust.

159. Defendants breached the fiduciary duties that they owed to Plaintiff and Class Members by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiff and Class Members.

160. Defendants' breach of fiduciary duty was a legal cause of damage to Plaintiff and Class Members.

161. But for Defendants' breach of fiduciary duty, the damage to Plaintiff and Class Members would not have occurred.

162. Defendants' breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and Class Members.

163. As a direct and proximate result of Defendants' breach of fiduciary duty, Plaintiff are entitled to and demand actual, consequential, and nominal damages and injunctive relief.

## COUNT IV
## DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
## (On Behalf of Plaintiff and the Class)

164. Plaintiff re-alleges and incorporate paragraphs 1-107 as if fully set forth herein.

165. 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.

166. Defendants owe duties of care to Plaintiff and Class Members which require them to adequately secure their PII.

167. Defendants still possess Plaintiff's and Class Members' PII.

168. Defendants do not specify in their Data Breach notification letters what steps they have taken to prevent a similar breach from occurring again.

169. Plaintiff 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.

170. 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 Plaintiff's and the Class Members' PII and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and the Class from further data breaches that compromise their PII.

171. Plaintiff 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 Plaintiff and Class Members for their respective lifetimes; and

h. Meaningfully educating Plaintiff 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.

172. The Court should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with the law and industry standards to protect Plaintiff's and Class Members' PII.

173. If an injunction is not issued, Plaintiff 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.

174. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. If another data breach occurs, Plaintiff and the Class will likely be subjected to fraud, identity theft, and other harms described herein. Contrarily, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is minimal given they have pre-existing legal obligations to employ these measures.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiff, 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, as defined herein, and appointing Plaintiff and his counsel to represent the Class;

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

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

i. prohibiting 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 Plaintiff's and Class Members' respective lifetimes;

iv. requiring Defendants to delete, destroy, and purge the PII of Plaintiff 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 Plaintiff 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 Plaintiff and Class Members;

vi. prohibiting Defendants from maintaining Plaintiff's 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 Plaintiff 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**

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

Date: May 15, 2023

Respectfully submitted,

*/s/ Randi Kassan*

RANDI KASSAN (Bar No.568656)
rkassan@milberg.com
**MILBERG, COLEMAN, BRYSON, PHILLIPS & GROSSMAN**
100 Garden City Plaza
Garden City, NY 11530
Telephone: (516) 741-5600

M. ANDERSON BERRY*
aberry@justice4you.com
GREGORY HAROUTUNIAN*
gharoutunian@justice4you.com
BRANDON P. JACK*
bjack@justice4you.com
**CLAYEO C. ARNOLD**
**A PROFESSIONAL LAW CORPORATION**
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829

*Attorneys for Plaintiff and the Proposed Class*

**Pro Hac Vice* forthcoming

# ClassAction.org



---