

Assigned for all purposes to: Spring Street Courthouse, Judicial Officer: David Cunningham III

1 **KAZEROUNI LAW GROUP, APC**  
 Abbas Kazerounian, Esq. (SBN: 249203)  
 2 ak@kazlg.com  
 Mona Amini, Esq. (SBN: 296829)  
 3 mona@kazlg.com  
 245 Fischer Avenue, Unit D1  
 4 Costa Mesa, California 92626  
 Telephone: (800) 400-6808  
 5 Facsimile: (800) 520-5523

6 *Attorneys for Plaintiff,*  
 7 *Natalie Nicholson*

8  
 9 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**  
 10 **FOR THE COUNTY OF LOS ANGELES – CIVIL COMPLEX**

11 NATALIE NICHOLSON, individually and on  
 12 behalf of all others similarly situated,

13 Plaintiff,

14 vs.

15 NONSTOP ADMINISTRATION AND  
 16 INSURANCE SERVICES, INC.,

17 Defendant.

Case No. **23STCV05512**

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

21 //  
 22 //  
 23 //  
 24 //  
 25 //  
 26 //  
 27 //



1 Plaintiff NATALIE NICHOLSON (“Plaintiff”), individually and on behalf of herself and  
2 the general public and all others similarly situated (“Class members”), by and through her attorneys,  
3 upon personal knowledge as to facts pertaining to herself and on information and belief as to all  
4 other matters, brings this class action against Defendant NONSTOP ADMINISTRATION AND  
5 INSURANCE SERVICES, INC (“Defendant” or “Nonstop”), and alleges as follows:

6 **NATURE OF THE CASE**

7 1. This is a data breach class action against Defendant and its related entities,  
8 subsidiaries, and agents for failing to secure and safeguard the personally identifiable information  
9 (“PII”) that Defendant collected and maintained and for failing to provide timely and adequate  
10 notice to Plaintiff and other Class members that their information had been stolen. Defendant works  
11 with partners to provide health benefits administrations services to employees and their family  
12 members. For its business purposes, Defendant collects, receives, and maintains a substantial  
13 amount of PII from individuals, like Plaintiff, through its servers and/or networks.

14 2. On or about February 15, 2023, Defendant issued a data breach notice letter to notify  
15 Plaintiff and similarly situated individuals of a data security incident that affected the security of  
16 their personal information. The data breach notice letter announced that an unknown party  
17 contacted Defendant and claimed to have accessed data from Defendant’s company. Defendant’s  
18 investigation determined that the unknown party accessed a cloud services platform maintained by  
19 Defendant without authorization on December 22, 2022 (the “Data Breach”). Defendant’s review of  
20 the information contained therein revealed that the information in Defendant’s cloud services  
21 platform included Plaintiff’s and other similarly situated individuals’ PII, including their name, date  
22 of birth, gender, address, email address, phone number, Social Security number, and health  
23 insurance provider name.

24 3. Although the Data Breach was identified in December 2022, placing sensitive  
25 customer information in the hands of malicious actors as a result of Defendant’s failure to safeguard  
26 Plaintiff’s and others’ PII, Defendant waited several months until on or around February 15, 2023  
27 to provide the data breach notice letter to Plaintiff and other similarly situated individuals. This  
28 notice was still lacking in information necessary for Plaintiff and Class members to understand the



1 scope and severity of the Data Breach. Further, due to this lapse in time between the Data Breach  
2 and Defendant's notice to affected individuals, unauthorized third parties have already been able to  
3 acquire and sell Plaintiff's and the Class members' PII on the black market or dark web, or  
4 otherwise fraudulently misuse it for their personal gain.

5 4. Defendant owed a duty to Plaintiff and Class members to implement and maintain  
6 reasonable and adequate security measures to secure, protect, and safeguard the PII it collected from  
7 individuals and maintained for business purposes and stored on its systems and networks, including  
8 its cloud services platform.

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, exfiltrated and/or disclosed to  
15 unauthorized persons. This action seeks to remedy these failings. Plaintiff brings this action on  
16 behalf of herself 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 herself  
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 is a  
25 California corporation that regularly 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 Los Angeles County, California. Plaintiff is an individual who was a customer of Defendant and was required to provide her personal information and PII to Defendant, and Plaintiff’s PII was 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, viewed, exfiltrated and/or disclosed to unauthorized persons in the Data Breach.

13. Defendant is a corporation formed under the laws of the state of California with its principal place of business and/or headquarters located at 1800 Sutter Street, Suite 730, Concord, California 94520.

**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.<sup>1</sup> 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.<sup>2</sup>

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

<sup>1</sup> 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).

<sup>2</sup> 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.”<sup>3</sup> 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.<sup>4</sup>

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.<sup>5</sup> This business has created a new market for the sale  
19 and purchase of this valuable data.<sup>6</sup>

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 <sup>3</sup> See Soma, *Corporate Privacy Trend, supra*.

26 <sup>4</sup> Risk Assessment Tool, Norton 2010, [www.everyclickmatters.com/victim/assessment-tool.html](http://www.everyclickmatters.com/victim/assessment-tool.html).

27 <sup>5</sup> 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 <sup>6</sup> 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.”<sup>7</sup>

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.<sup>8</sup>

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.”<sup>9</sup>

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.<sup>10</sup> 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 <sup>7</sup> 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 <sup>8</sup> 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).

<sup>9</sup> California Data Breach Report, Kamala D. Harris, Attorney General, California Department  
of Justice, February 2016.

<sup>10</sup> See GAO, GAO Report 9 (2007) available at <http://www.gao.gov/new.items/d07737.pdf>.

1           26. In addition, the GAO Report states that victims of identity theft will face “substantial  
2 costs and inconveniences repairing damage to their credit records ... [and their] good name.”  
3 According to the FTC, identity theft victims must spend countless hours and large amounts of  
4 money repairing the impact to their good name and credit record.<sup>11</sup>

5           27. Identity thieves use personal information for a variety of crimes, including credit  
6 card fraud, phone or utilities fraud, and bank/finance fraud.<sup>12</sup> According to Experian, “[t]he research  
7 shows that personal information is valuable to identity thieves, and if they can get access to it, they  
8 will use it” to among other things: open a new credit card or loan; change a billing address so the  
9 victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and  
10 write bad checks; use a debit card number to withdraw funds; obtain a new driver’s license or ID;  
11 use the victim’s information in the event of arrest or court action.<sup>13</sup>

12           28. Social Security numbers, for example, are among the worst kind of personal  
13 information to have stolen because they may be put to a variety of fraudulent uses and are difficult  
14 for an individual to change. The Social Security Administration stresses that the loss of an  
15 individual’s Social Security number, as is the case here, can lead to identity theft and extensive  
16 financial fraud:

17           A dishonest person who has your Social Security number can use it to get  
18 other personal information about you. Identity thieves can use your  
19 number and your good credit to apply for more credit in your name. Then,  
20 they use the credit cards and don’t pay the bills, it damages your credit.  
21 You may not find out that someone is using your number until you’re  
22 turned down for credit, or you begin to get calls from unknown creditors  
23 demanding payment for items you never bought. Someone illegally using

23 <sup>11</sup> See FTC Identity Theft Website: <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>.

24 <sup>12</sup> The FTC defines identity theft as “a fraud committed or attempted using the identifying  
25 information of another person without authority.” 16 C.F.R. § 603.2. The FTC describes  
26 “identifying information” as “any name or number that may be used, alone or in conjunction with  
27 any other information, to identify a specific person,” including, among other things, “[n]ame, social  
28 security number, date of birth, official State or government issued driver's license or identification  
29 number, alien registration number, government passport number, employer, or taxpayer  
30 identification number.” *Id.*

31 <sup>13</sup> See Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How  
32 Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), available at  
33 [https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-  
34 information-and-how-can-you-protect-yourself/](https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/).



1 your Social Security number and assuming your identity can cause a lot of  
2 problems.<sup>14</sup>

3 29. According to the IBM and Ponemon Institute’s 2019 “Cost of a Data Breach” report,  
4 the average cost of a data breach per consumer was \$150 per record.<sup>15</sup> Other estimates have placed  
5 the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity  
6 theft – a common result of data breaches – was \$298 dollars.<sup>16</sup> And in 2019, Javelin Strategy &  
7 Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket  
8 cost to consumers for identity theft was \$375.<sup>17</sup>

9 30. A person whose PII has been compromised may not see any signs of identity theft  
10 for years. According to the GAO Report:

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

17 31. For example, in 2012, hackers gained access to LinkedIn’s users’ passwords.  
18 However, it was not until May 2016, four years after the breach, that hackers released the stolen  
19 email and password combinations.<sup>18</sup>

20 32. It is within this context that Plaintiff and thousands of similarly situated individuals  
21 must now live with the knowledge that their PII is forever in cyberspace and was taken by  
22 unauthorized persons willing to use the information for any number of improper purposes and  
23 scams, including making the information available for sale on the dark web and/or the black market.

24 <sup>14</sup> 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>.

25 <sup>15</sup> Brook, *What’s the Cost of a Data Breach in 2019*, *supra*.

26 <sup>16</sup> Norton By Symantec, 2013 Norton Report 8 (2013), *available at* [https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton\\_raportti.pdf](https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf).

27 <sup>17</sup> 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).

28 <sup>18</sup> 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 PII***

33. Defendant represents that it understands the importance of protecting such information. For example, in its Privacy Statement, Defendant states that “Personally identifiable patient, physician, and Your information shall remain confidential and not be released,” and that it uses “regulatory-compliant security measures to protect the information.”<sup>19</sup>

34. Defendant further represents that “We offer and provide the Company Site and Our products and services in a manner that complies with all applicable laws and regulations we are aware of and become known to us and will continue to do so.”<sup>20</sup>

35. Defendant’s Privacy Statement states that it obtains information “through the Company Information Site by using forms posted on or linked to the site that seek information, including Your interests and concerns, preferences for products and services, or contact information. We also seek information through email and in other routine, lawful operations that We conduct in the ordinary course of operating Our business. These operations may include the use of standard data gathering functionality, such as cookies and other devices that collect certain standard information generated by Web browsers about users of the Company Site, such as IP addresses, access times, and their experience using one or more web sites operated by or on behalf of Us.”<sup>21</sup>

***The Data Breach***

36. On or around February 15, 2023 Defendant issued a data breach notice letter to Plaintiff and other similarly situated individuals who were victims of the Data Breach announcing that an unknown party contacted Defendant and claimed to have accessed data from Defendant’s company. Defendant’s investigation determined that the unknown party accessed a cloud services platform maintained by Defendant without authorization on December 22, 2022 (the “Data Breach”). Defendant’s review of the information contained therein revealed that the information in Defendant’s cloud services platform included Plaintiff’s and other similarly situated individuals’

<sup>19</sup> See <https://www.nonstophealth.com/privacy/>

<sup>20</sup> *Id.*

<sup>21</sup> *Id.*

1 PII, including their name, date of birth, gender, address, email address, phone number, Social  
2 Security number, and health insurance provider name.

3 37. According to Defendant, revealed that the information in Defendant's cloud services  
4 platform included Plaintiff's and other similarly situated individuals' PII, including their name, date  
5 of birth, gender, address, email address, phone number, Social Security number, and health  
6 insurance provider name.

7 38. Defendant's Data Breach notice letter provided little other information regarding the  
8 Data Breach itself. For instance, Defendant provided no information regarding how the breach  
9 occurred, why it waited months since learning of the data breach and identifying Plaintiff and other  
10 affected individuals to send them notice, what happened to Plaintiff's and the Class members' PII,  
11 or how many people were affected by the Data Breach.

12 39. As a result of the Data Breach, Plaintiff has suffered an invasion and loss of  
13 Plaintiff's privacy, including learning that her PII has been detected on the dark web, Plaintiff has  
14 spent money purchasing credit monitoring and/or identity theft protection, and Plaintiff has spent  
15 additional personal time monitoring Plaintiff's financial accounts, which was time that Plaintiff  
16 otherwise would have spent performing other activities or leisurely events for the enjoyment of life  
17 rather than mitigating the impact of the Data Breach.

18 40. As a result of the Data Breach, Plaintiff is and will continue to be at heightened risk  
19 for financial fraud and/or identity theft, and the associated damages resulting from it, for years to  
20 come.

21 ***Defendant Knew or Should Have Known PII Are High Risk Targets***

22 41. Defendant knew or should have known that PII like that at issue here, is a high-risk  
23 target for identity thieves.

24  
25  
26  
27  
28



1           42.     The Identity Theft Resource Center reported that the banking/credit/financial sector  
2 had the third largest number of breaches in 2018. According to the ITRC this sector suffered 135  
3 data breaches exposing at least 1,709,013 million records in 2018.<sup>22</sup>

4           43.     Prior to the breach there were many reports of high-profile data breaches that should  
5 have put a company like Defendant on high alert and forced it to closely examine its own security  
6 procedures, as well as those of third parties with which it did business and gave access to its  
7 subscriber PII. Notable breaches included Capital One, which announced that in March 2019 a  
8 hacker had gained access to 100 million U.S. customer accounts and credit card applications.  
9 Similarly, in May 2019, First American Financial reported a security incident on its website that  
10 potentially exposed 885 million real estate and mortgage related documents, among others. Across  
11 industries, financial services have the second-highest cost per breached record, behind healthcare. In  
12 financial services, an average breach costs \$210 per record, while a “mega breach,” like Capital  
13 One’s, can cost up to \$388 per record.<sup>23</sup>

14           44.     Anurag Kahol, CTO of Bitglass recently commented that “[g]iven that organizations  
15 in the financial services industry are entrusted with highly valuable, personally identifiable  
16 information (PII), they represent an attractive target for cybercriminals[.]” HelpNetSecurity reports  
17 that “[h]acking and malware are leading the charge against financial services and the costs  
18 associated with breaches are growing. Financial services organizations must get a handle on data  
19 breaches and adopt a proactive security strategy if they are to properly protect data from an  
20 evolving variety of threats.”<sup>24</sup>

21           45.     As such, Defendant was aware that PII is at high risk of theft, and consequently  
22 should have but did not take appropriate and standard measures to protect Plaintiff’s and Class  
23

24  
25 <sup>22</sup> 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](https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf).

26 <sup>23</sup> 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 <sup>24</sup> 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 members' PII against cyber-security attacks that Defendant should have anticipated and guarded  
2 against.

3 **CLASS ACTION ALLEGATIONS**

4 46. Pursuant to Cal. Code Civ. Proc. § 382 and Cal. Civ. Code § 1781, Plaintiff seeks to  
5 represent and intends to seek certification of a class (the "Class") defined as:

6 ***All California residents whose PII was subjected to the Data Breach.***

7 47. Excluded from the Class are: (1) Defendant and its officers, directors, employees,  
8 principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents,  
9 affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such  
10 persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of  
11 their immediate families.

12 48. Certification of Plaintiff's claims for class wide treatment is appropriate because  
13 Plaintiff can prove the elements of their claims on a class wide basis using the same evidence as  
14 would be used to prove those elements in individual actions alleging the same claims.

15 49. The Class members are so numerous and geographically dispersed throughout  
16 California that joinder of all Class members would be impracticable. While the exact number of  
17 Class members is unknown, based on information and belief, the Class consists of tens of thousands  
18 of Defendant's individuals in California, including Plaintiff and the Class members. Plaintiff  
19 therefore believes that the Class is so numerous that joinder of all members is impractical.

20 50. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed  
21 members of the Class, had their PII compromised in the Data Breach. Plaintiff and Class members  
22 were injured by the same wrongful acts, practices, and omissions committed by Defendant, as  
23 described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that  
24 give rise to the claims of all Class members.

25 51. There is a well-defined community of interest in the common questions of law and  
26 fact affecting Class members. The questions of law and fact common to Class members  
27 predominate over questions affecting only individual Class members, and include without  
28 limitation:

1 (a) Whether Defendant had a duty to implement and maintain reasonable security  
2 procedures and practices appropriate to the nature of the PII it collected, stored, and maintained  
3 from Plaintiff and Class members;

4 (b) Whether Defendant breached its duty to protect the PII of Plaintiff and each Class  
5 member; and

6 (c) Whether Plaintiff and each Class member are entitled to damages and other equitable  
7 relief.

8 52. Plaintiff will fairly and adequately protect the interests of the Class members.  
9 Plaintiff is an adequate representative of the Class in that Plaintiff has no interests adverse to or that  
10 conflicts with the Class Plaintiff seeks to represent. Plaintiff has retained counsel with substantial  
11 experience and success in the prosecution of complex consumer protection class actions of this  
12 nature.

13 53. A class action is superior to any other available method for the fair and efficient  
14 adjudication of this controversy since individual joinder of all Class members is impractical.  
15 Furthermore, the expenses and burden of individual litigation would make it difficult or impossible  
16 for the individual members of the Class to redress the wrongs done to them, especially given that  
17 the damages or injuries suffered by each individual member of the Class are outweighed by the  
18 costs of suit. Even if the Class members could afford individualized litigation, the cost to the court  
19 system would be substantial and individual actions would also present the potential for inconsistent  
20 or contradictory judgments. By contrast, a class action presents fewer management difficulties and  
21 provides the benefits of single adjudication and comprehensive supervision by a single court.

22 54. Defendant has acted or refused to act on grounds generally applicable to the entire  
23 Class, thereby making it appropriate for this Court to grant final injunctive, including public  
24 injunctive relief, and declaratory relief with respect to the Class as a whole.

25  
26  
27  
28



**CAUSES OF ACTION**

**FIRST CAUSE OF ACTION**

**Violation of the California Consumer Privacy Act of 2018 (“CCPA”)**

**Cal. Civ. Code §§ 1798.100, *et seq.***

55. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

56. 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 protect it from unauthorized access. The California Legislature explained: “The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm.”<sup>25</sup>

57. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

58. It also requires “[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party 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.” 1798.81.5(c).

<sup>25</sup> California Consumer Privacy Act (CCPA) Compliance, <https://buyergenomics.com/ccpa-compliance/>.





1           59. Section 1798.150(a)(1) of the CCPA provides: “Any consumer whose nonencrypted  
2 or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access  
3 and exfiltration, theft, or disclosure as a result of the business’ violation of the duty to implement  
4 and maintain reasonable security procedures and practices appropriate to the nature of the  
5 information to protect the personal information may institute a civil action for” statutory or actual  
6 damages, injunctive or declaratory relief, and any other relief the court deems proper.

7           60. Plaintiff and Class members are “consumer[s]” as defined by Civ. Code  
8 § 1798.140(g) because they are “natural person[s] who [are] California resident[s], as defined in  
9 Section 17014 of Title 18 of the California Code of Regulations, as that section read on September  
10 1, 2017.”

11           61. Defendant is a “business” as defined by Civ. Code § 1798.140(c) because Defendant:

12           a) is a “sole proprietorship, partnership, limited liability company, corporation,  
13 association, or other legal entity that is organized or operated for the profit or financial benefit  
14 of its shareholders or other owners”;

15           b) “collects consumers’ personal information, or on the behalf of which is collected  
16 and that alone, or jointly with others, determines the purposes and means of the processing of  
17 consumers’ personal information”;

18           c) does business in and is headquartered in California; and

19           d) has annual gross revenues in excess of \$25 million; annually buys, receives for  
20 the business’ commercial purposes, sells or shares for commercial purposes, alone or in  
21 combination, the personal information of 50,000 or more consumers, households, or devices; or  
22 derives 50 percent or more of its annual revenues from selling consumers’ personal  
23 information.

24           62. The PII accessed and taken by unauthorized persons in the Data Breach is “personal  
25 information” as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff’s and other  
26 Class members’ unencrypted names, addresses, loan account numbers, and Social Security  
27 numbers, among other personal information.

28





1           69. In the course of conducting its business, Defendant committed “unlawful” business  
2 practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee,  
3 manage, monitor and audit appropriate data security processes, controls, policies, procedures,  
4 protocols, and software and hardware systems to safeguard and protect Plaintiff’s and Class  
5 members’ PII, and by violating the statutory and common law alleged herein, including, *inter alia*,  
6 California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100, *et seq.*) and Article I,  
7 Section 1 of the California Constitution (California’s constitutional right to privacy) and Civil Code  
8 § 1798.81.5. Plaintiff and Class members reserve the right to allege other violations of law by  
9 Defendant constituting other unlawful business acts or practices. Defendant’s above-described  
10 wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this  
11 date.

12           70. Defendant also violated the UCL by failing to timely notify Plaintiff and Class  
13 members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of  
14 their PII. If Plaintiff and Class members had been notified in an appropriate fashion, they could  
15 have taken precautions to better safeguard and protect their PII.

16           71. Defendant’s above-described wrongful actions, inaction, omissions, want of ordinary  
17 care, misrepresentations, practices, and non-disclosures also constitute “unfair” business acts and  
18 practices in violation of the UCL in that Defendant’s wrongful conduct is substantially injurious to  
19 consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and  
20 unscrupulous. Defendant’s practices are also contrary to legislatively declared and public policies  
21 that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize  
22 appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the  
23 California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant’s wrongful  
24 conduct outweighs any alleged benefits attributable to such conduct. There were reasonably  
25 available alternatives to further Defendant’s legitimate business interests other than engaging in the  
26 above-described wrongful conduct.





1           72. The UCL also prohibits any “fraudulent business act or practice.” Defendant’s  
2 above-described claims, nondisclosures and misleading statements were false, misleading, and  
3 likely to deceive the consuming public in violation of the UCL.

4           73. As a direct and proximate result of Defendant’s above-described wrongful actions,  
5 inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach  
6 and its violations of the UCL, Plaintiff and Class members have suffered (and will continue to  
7 suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an  
8 imminent, immediate and the continuing increased risk of identity theft and identity fraud – risks  
9 justifying expenditures for protective and remedial services for which they are entitled to  
10 compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) statutory  
11 damages under the CCPA, (v) deprivation of the value of their PII for which there is a well-  
12 established national and international market, and/or (vi) the financial and temporal cost of  
13 monitoring their credit, monitoring financial accounts, and mitigating damages.

14           74. Unless restrained and enjoined, Defendant will continue to engage in the above-  
15 described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of  
16 herself, the Class members, and the general public, also seeks restitution and an injunction,  
17 including public injunctive relief prohibiting Defendant from continuing such wrongful conduct,  
18 and requiring Defendant to modify its corporate culture and design, adopt, implement, control,  
19 direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies,  
20 procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted  
21 to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code  
22 § 17203.

23 //  
24 //  
25 //  
26 //  
27 //  
28 //

1 **THIRD CAUSE OF ACTION**

2 **Breach of Contract**

3 75. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully  
4 set forth herein.

5 76. Plaintiff and Class members entered into express contracts with Defendant that  
6 included Defendant’s promise to protect nonpublic personal information given to Defendant or that  
7 Defendant gathered on its own, from unauthorized disclosure.

8 77. Plaintiff and Class members performed their obligations under the contracts,  
9 including Defendant’s Terms of Use and/or privacy policy when they provided their PII to  
10 Defendant in connection with Defendant’s products and services.

11 78. Defendant breached its contractual obligation to protect the nonpublic personal  
12 information Defendant gathered when the information was exposed as part of the Data Breach.

13 79. As a direct and proximate result of the Data Breach, Plaintiff and Class members  
14 have been harmed and have suffered, and will continue to suffer, damages and injuries.

15 **PRAYER FOR RELIEF**

16 **WHEREFORE**, Plaintiff, on behalf of herself individually as well as all members of the  
17 Class respectfully requests that (i) this action be certified as a class action, (ii) Plaintiff each be  
18 designated a representative of the Class, (iii) Plaintiff’s counsel be appointed as counsel for the  
19 Class. Plaintiff, on behalf of herself and members of the Class further request that upon final trial or  
20 hearing, judgment be awarded against Defendant for:

- 21 (i) actual and punitive damages to be determined by the trier of fact;
- 22 (ii) equitable relief, including restitution;
- 23 (iii) pre- and post-judgment interest at the highest legal rates applicable;
- 24 (iv) appropriate injunctive relief;
- 25 (v) attorneys’ fees and litigation expenses under Code of Civil Procedure  
26 § 1021.5 and other applicable law;
- 27 (vi) costs of suit; and
- 28 (vii) such other and further relief the Court deems just and proper.



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**DEMAND FOR JURY TRIAL**

Plaintiff hereby demands a jury trial on all issues so triable.

Respectfully submitted,

Dated: March 13, 2023

**KAZEROUNI LAW GROUP, APC**

By:   
\_\_\_\_\_  
ABBAS KAZEROUNIAN, ESQ.  
MONA AMINI, ESQ.

*Attorneys for Plaintiff*

