

1 Adam J Schwartz (SBN 251831)  
2 e-service: adam@ajschwartz.com  
3 ADAM J SCHWARTZ, ATTORNEY AT LAW  
4 5670 Wilshire Blvd., Suite 1800  
5 Los Angeles, CA 90036  
6 phone: (323) 455-4016

7 *Attorney for JOHN BLUMENSTOCK, THOMAS*  
8 *ROSSELLO, and JEFFREY BRANCH and*  
9 *proposed class*

10 UNITED STATES DISTRICT COURT  
11 NORTHERN DISTRICT OF CALIFORNIA  
12 SAN FRANCISCO DIVISION

13 JOHN BLUMENSTOCK, THOMAS  
14 ROSSELLO, and JEFFREY BRANCH on  
15 behalf of themselves and all others similarly  
16 situated,

17 Plaintiffs,

v.

18 ETHOS TECHNOLOGIES, INC.,  
19 Defendant.

Case No. 3:23-cv-00073

**CLASS ACTION COMPLAINT FOR  
DAMAGES**

**JURY TRIAL DEMANDED**

20 Plaintiffs, John Blumenstock, Thomas Rossello, and Jeffrey Branch, through their  
21 attorneys, bring this Class Action Complaint against the Defendant, Ethos Technologies, Inc.  
22 (“Ethos” or “Defendant”), alleging as follows:

**INTRODUCTION**

23 1. From August to December 2022, Ethos, an online life insurance company, lost  
24 control over thousands of consumers’ Social Security numbers during a four-month data breach  
25 by cybercriminals (“Data Breach”).

26 2. Ethos’ breach differs from typical data breaches because it affects consumers who  
27 had no relationship with Ethos, never sought one, and never consented to Ethos collecting and  
28 storing their information.

///

1           3.       Ethos sourced their information from third parties, stored it on Ethos’ systems,  
2 and assumed a duty to protect it, advertising that Ethos “consider[s] safeguarding the security  
3 and privacy of customer data an integral part of our mission.” But Ethos never implemented the  
4 security safeguards needed to fulfill that duty.

5           4.       Indeed, Ethos has suffered two data breaches in less than a year, allowing hackers  
6 to exploit the *same* vulnerabilities in its systems twice.

7           5.       The first breach spanned from July 2021 through January 2022, in which hackers  
8 bypassed Ethos’ cybersecurity to steal consumers’ driver’s license numbers.

9           6.       They did so by inputting basic information about consumers from public sources  
10 on Ethos’ website to generate insurance quotes. Hackers could generate a quote with as little as a  
11 consumer’s name, date, and address.

12           7.       In response, Ethos’ system would retrieve information collected from its third-  
13 party sources and return a report with expanded information on the consumer, including their  
14 driver’s license number.

15           8.       Ethos then stored that information in its source code, code Ethos left unprotected  
16 and accessible to outsiders like hackers.

17           9.       Using “tools,” hackers could then extract consumer information from Ethos’  
18 source code.

19           10.      In other words, with basic information on a person’s background, hackers could  
20 request their driver’s license numbers from Ethos and then capture it from Ethos’ website—no  
21 matter whether the person had a relationship with Ethos, wanted one, or consented to Ethos using  
22 their personal information.

23           11.      Ethos learned about the first data breach in January 2022, after hackers had  
24 already been farming its systems for consumers’ driver’s license numbers for five months.

25           12.      Even so, Ethos did not remedy the security vulnerability, leading to an even worse  
26 data breach seven months later.

27           13.      In August 2022, hackers used the same method to request quotes and retrieve  
28 consumers’ *Social Security numbers*.





1           30. But, on information and belief, Ethos did not implement those security measures  
2 as advertised, nor were they reasonably sufficient to protect the highly sensitive data Ethos  
3 collected.

4           31. As Plaintiffs allege above, Ethos collects data on individuals who have no  
5 relationship with it, do not want one, and have never consented to its services.

6           32. It does so by sourcing that information from third parties, “such as private sources  
7 (insurance agents, consumer reporting agencies, healthcare providers, health information  
8 exchanges, and other data providers)[.]” Those “private sources” supply Ethos data concerning  
9 all aspects of consumers’ lives, including their health data, familial details, credit scores, location  
10 data, “sensory data” on their voices, and “Government-issued identification data,” like their  
11 driver’s license and Social Security numbers.<sup>1</sup>

12           33. Ethos designed its website to allow anyone with a consumer’s basic information  
13 to apply for Ethos insurance policies, using as little as their name, address, and birth date.

14           34. After receiving an application, Ethos retrieves information on the consumer from  
15 its third-party sources, then storing it on its website’s source code.

16           35. But despite centering its business model on its website portal, it never secured the  
17 highly sensitive information it collects and stores on that portal.

18           36. As a result, hackers could exploit that vulnerability and steal consumers’  
19 information. And they did so twice.

20           **B. Ethos Fails to Safeguard Consumer PII**

21           37. From August 2021 through January 2022, hackers exploited the vulnerability to  
22 steal 13,300 consumers’ driver’s license numbers.

23           38. Ethos did not detect the hack until January 2022, allowing hackers to pilfer  
24 consumers’ PII for five months.

25           39. After detecting the hack, Ethos investigated it and discovered its vulnerability.  
26 See attached **Exhibit A** for Ethos’ breach notice regarding the driver’s license number breach.  
27

28 <sup>1</sup> See Ethos’ privacy policy at <https://www.ethoslife.com/privacy/> (last accessed January 2, 2023).

1           40.     But even though Ethos discovered the vulnerability and its impact on consumers,  
2 Ethos did not fix the problem.

3           41.     Indeed, just seven months later hackers exploited the same vulnerability again,  
4 causing an even worse breach.

5           42.     In August 2022, hackers used the same techniques to steal consumers' Social  
6 Security numbers.

7           43.     And again, Ethos did not detect the hack when it happened, nor would it for four  
8 months.

9           44.     By that time, the damage was done, and hackers had stolen the Social Security  
10 numbers belonging to thousands of individuals.

11           45.     Plaintiffs Blumenstock, Rossello, and Branch are individuals and Data Breach  
12 victims. They have no relationship with Ethos, never sought one, and never consented to the  
13 company using or storing their PII.

14           46.     Even though plaintiffs never had a relationship with Ethos, it still collected their  
15 PII and stored it in Ethos' computer systems.

16           47.     In collecting and maintaining the PII, Ethos assumed a duty to safeguard it  
17 according to its internal policies and state and federal law.

18           48.     On information and belief, Ethos failed to adequately train its employees on  
19 reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose  
20 control over consumer PII twice through the same security vulnerability. Ethos' negligence is  
21 evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII in  
22 two data breaches arising from the same problem. Further, Ethos' multiple breach notices make  
23 clear that Ethos cannot, or will not, protect the PII it retrieves and possesses on consumers.  
24 Attached as **Exhibit B** is a copy of Ethos' second breach notice disclosing the Data Breach  
25 affecting consumers' Social Security numbers.

26           49.     Indeed, even Ethos recognizes the threat its Data Breach poses in its breach  
27 notice. It offered breach victims credit monitoring and "urged" them to guard themselves against  
28 the "potential misuse of information": "we urge you to remain vigilant for incidents of potential

1 fraud and identity theft, including by regularly reviewing account statements and monitoring  
2 your credit reports.”

3 **C. Plaintiffs’ Experiences**

4 **i. Plaintiff Blumenstock.**

5 50. Plaintiff Blumenstock is an individual and data breach victim.

6 51. Despite never forming or seeking a relationship with Ethos, Plaintiff  
7 Blumenstock’s PII was compromised in Ethos’ second data breach, compromising his Social  
8 Security number and exposing him to identity theft and fraud.

9 52. Indeed, around two weeks after the Data Breach, criminals used his PII to steal  
10 \$6,800 from his Wells Fargo account.

11 53. Plaintiff Blumenstock does not recall ever learning that his information was  
12 compromised in a data breach incident, other than the breach at issue in this case.

13 54. As a result of the Data Breach and the recommendations of Defendant’s Notice,  
14 Plaintiff Blumenstock made reasonable efforts to mitigate the impact of the Data Breach,  
15 including but not limited to researching the Data Breach, reviewing credit card and financial  
16 account statements, changing his online account passwords, placing a credit freeze through the  
17 three main credit bureaus, and monitoring his credit information as suggested by Defendant.

18 55. Indeed, Plaintiff Blumenstock has spent considerable time reaching out to  
19 Experian, the designated contact organization for the Ethos Data Breach Response Plan. The  
20 information provided by Experian was limited and unable to address Plaintiff Blumenstock’s  
21 concerns.

22 56. Plaintiff Blumenstock has spent approximately five hours responding to the Data  
23 Breach and will continue to spend valuable time he otherwise would have spent on other  
24 activities, including but not limited to work and/or recreation.

25 57. Plaintiff Blumenstock has and will spend considerable time and effort monitoring  
26 his accounts to protect himself from identity theft. Plaintiff Blumenstock fears for his personal  
27 financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff  
28 Blumenstock has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and

1 frustration because of the Data Breach. This goes far beyond allegations of mere worry or  
2 inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law  
3 contemplates and addresses.

4 58. Plaintiff Blumenstock is now subject to the present and continuing risk of fraud,  
5 identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third  
6 parties. This injury was worsened by Defendant's delay in informing Plaintiffs and Class  
7 Members about the Data Breach.

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

11 **ii. Plaintiff Rossello**

12 60. Plaintiff Rossello is an individual and data breach victim.

13 61. Despite never forming or seeking a relationship with Ethos, Plaintiff Rossello's  
14 PII was compromised in the Data Breach, compromising his Social Security number and  
15 exposing him to identity theft and fraud.

16 62. Indeed, following the Data Breach, Mr. Rossello suffered identity theft and fraud  
17 repeatedly, including the following instances: (i) Bank of America called him to verify a  
18 payment card someone tried to open in his name without his authorization; (ii) He received a  
19 similar call from JP Morgan Chase seeking to verify a credit card he never opened or authorized;  
20 (iii) These instances prompted him to review his credit report, where he saw a hard inquiry from  
21 Pentagon Credit Union that he did not authorize. After investigating the inquiry, he learned that  
22 someone had tried to open a credit card in his name; and (iv) He learned that criminals had tried  
23 to open a credit card in his name 13 times with Check Systems, attempts he never authorized.

24 63. Given these attempts, Plaintiff Rossello contacted all credit bureaus to freeze his  
25 accounts, also contacting his phone provider to lock his phone account. In total, Plaintiff  
26 Rossello has devoted 30 hours to remediating the fraud he has suffered.

27 64. Plaintiff Rosello does not recall ever learning that his information was  
28 compromised in a data breach incident, other than the breach at issue in this case.

1           65. As a result of the Data Breach and the recommendations of Defendant’s Notice,  
2 Plaintiff Rossello made reasonable efforts to mitigate the impact of the Data Breach, including  
3 but not limited to researching the Data Breach, reviewing credit card and financial account  
4 statements, changing his online account passwords, and monitoring his credit information as  
5 suggested by Defendant.

6           66. Plaintiff Rossello has and will spend considerable time and effort monitoring his  
7 accounts to protect himself from identity theft. Plaintiff Rossello fears for his personal financial  
8 security and uncertainty over what PII was exposed in the Data Breach. Plaintiff Rossello has  
9 and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of  
10 the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly  
11 the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

12           67. Plaintiff Rossello is now subject to the present and continuing risk of fraud,  
13 identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third  
14 parties. This injury was worsened by Defendant’s delay in informing Plaintiffs and Class  
15 Members about the Data Breach.

16           68. Plaintiff Rossello has a continuing interest in ensuring that his PII, which, upon  
17 information and belief, remains backed up in Defendant’s possession, is protected and  
18 safeguarded from future breaches.

19           **iii. Plaintiff Branch**

20           69. Plaintiff Branch is an individual and data breach victim.

21           70. Despite never forming or seeking a relationship with Ethos, Plaintiff Branch’s PII  
22 was compromised in Ethos’ second data breach, compromising his Social Security number and  
23 exposing him to identity theft and fraud.

24           71. Indeed, following the data breach, unauthorized individuals opened two bank  
25 accounts in Plaintiff Branch’s name at the First National Bank of Omaha, then accessing other  
26 accounts belonging to him to transfer around \$60,000 from his accounts to fraudulent accounts, a  
27 devastating financial loss. As a result, he has spent two days attempting to remediate the harm  
28 this identity theft and fraud has caused him.

1           72. Plaintiff Branch does not recall ever learning that his information was  
2 compromised in a data breach incident, other than the breach at issue in this case.

3           73. As a result of the Data Breach and the recommendations of Defendant’s Notice,  
4 Plaintiff Branch made reasonable efforts to mitigate the impact of the Data Breach, including but  
5 not limited to researching the Data Breach, reviewing credit card and financial account  
6 statements, changing his online account passwords, and monitoring his credit information as  
7 suggested by Defendant.

8           74. Plaintiff Branch has and will spend considerable time and effort monitoring his  
9 accounts to protect himself from identity theft. Plaintiff Branch fears for his personal financial  
10 security and uncertainty over what PII was exposed in the Data Breach. Plaintiff Branch has and  
11 is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the  
12 Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the  
13 sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

14           75. Plaintiff Branch is now subject to the present and continuing risk of fraud, identity  
15 theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties.  
16 This injury was worsened by Defendant’s delay in informing Plaintiffs and Class Members about  
17 the Data Breach.

18           76. Plaintiff Branch has a continuing interest in ensuring that his PII, which, upon  
19 information and belief, remains backed up in Defendant’s possession, is protected and  
20 safeguarded from future breaches.

21           **D. Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity**  
22 **Theft**

23           77. Plaintiffs and members of the proposed Class have suffered injury from the  
24 misuse of their PII that can be directly traced to Defendant.

25           78. As a result of Ethos’ failure to prevent the Data Breach, Plaintiffs and the  
26 proposed Class have suffered and will continue to suffer damages, including monetary losses,  
27 lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of  
28 suffering:

- 1 a. The loss of the opportunity to control how their PII is used;
- 2 b. The diminution in value of their PII;
- 3 c. The compromise and continuing publication of their PII;
- 4 d. Out-of-pocket costs associated with the prevention, detection, recovery, and
- 5 remediation from identity theft or fraud;
- 6 e. Lost opportunity costs and lost wages associated with the time and effort
- 7 expended addressing and attempting to mitigate the actual and future
- 8 consequences of the Data Breach, including, but not limited to, efforts spent
- 9 researching how to prevent, detect, contest, and recover from identity theft and
- 10 fraud;
- 11 f. Delay in receipt of tax refund monies;
- 12 g. Unauthorized use of stolen PII; and
- 13 h. The continued risk to their PII, which remains in the possession of defendant and
- 14 is subject to further breaches so long as defendant fails to undertake the
- 15 appropriate measures to protect the PII in their possession.

16 79. Stolen PII is one of the most valuable commodities on the criminal information  
17 black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to  
18 \$1,000.00 depending on the type of information obtained.

19 80. The value of Plaintiffs' and the proposed Class's PII on the black market is  
20 considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen  
21 private information openly and directly on various "dark web" internet websites, making the  
22 information publicly available, for a substantial fee of course.

23 81. It can take victims years to spot identity or PII theft, giving criminals plenty of  
24 time to use that information for cash.

25 82. One such example of criminals using PII for profit is the development of "Fullz"  
26 packages.

27 83. Cyber-criminals can cross-reference two sources of PII to marry unregulated data  
28 available elsewhere to criminally stolen data with an astonishingly complete scope and degree of

1 accuracy in order to assemble complete dossiers on individuals. These dossiers are known as  
2 “Fullz” packages.

3 84. The development of “Fullz” packages means that stolen PII from the Data Breach  
4 can easily be used to link and identify it to Plaintiffs’ and the proposed Class’s phone numbers,  
5 email addresses, and other unregulated sources and identifiers. In other words, even if certain  
6 information such as emails, phone numbers, or credit card numbers may not be included in the  
7 PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package  
8 and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam  
9 telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the  
10 proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find  
11 that Plaintiffs’ and other members of the proposed Class’s stolen PII is being misused, and that  
12 such misuse is fairly traceable to the Data Breach.

13 85. Defendant disclosed the PII of Plaintiffs and members of the proposed Class for  
14 criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed,  
15 and exposed the PII of Plaintiffs and members of the proposed Class to people engaged in  
16 disruptive and unlawful business practices and tactics, including online account hacking,  
17 unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial  
18 accounts (i.e., identity fraud), all using the stolen PII.

19 86. Defendant’s failure to properly notify Plaintiffs and members of the proposed  
20 Class of the Data Breach exacerbated Plaintiffs’ and members of the proposed Class’s injury by  
21 depriving them of the earliest ability to take appropriate measures to protect their PII and take  
22 other necessary steps to mitigate the harm caused by the Data Breach.

23 **E. Defendant failed to adhere to FTC guidelines.**

24 87. According to the Federal Trade Commission (“FTC”), the need for data security  
25 should be factored into all business decision-making. To that end, the FTC has issued numerous  
26 guidelines identifying best data security practices that businesses, such as Defendant, should  
27 employ to protect against the unlawful exposure of PII.

28 ///

1 88. In 2016, the FTC updated its publication, Protecting Personal Information: A  
2 Guide for Business, which established guidelines for fundamental data security principles and  
3 practices for business. The guidelines explain that businesses should:

- 4 a. protect the personal customer information that they keep;
- 5 b. properly dispose of personal information that is no longer needed;
- 6 c. encrypt information stored on computer networks;
- 7 d. understand their network’s vulnerabilities; and
- 8 e. implement policies to correct security problems.

9 89. The guidelines also recommend that businesses watch for large amounts of data  
10 being transmitted from the system and have a response plan ready in the event of a breach.

11 90. The FTC recommends that companies not maintain information longer than is  
12 needed for authorization of a transaction; limit access to sensitive data; require complex  
13 passwords to be used on networks; use industry-tested methods for security; monitor for  
14 suspicious activity on the network; and verify that third-party service providers have  
15 implemented reasonable security measures.

16 91. The FTC has brought enforcement actions against businesses for failing to  
17 adequately and reasonably protect customer data, treating the failure to employ reasonable and  
18 appropriate measures to protect against unauthorized access to confidential consumer data as an  
19 unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”),  
20 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must  
21 take to meet their data security obligations.

22 92. Defendant’s failure to employ reasonable and appropriate measures to protect  
23 against unauthorized access to consumers’ PII constitutes an unfair act or practice prohibited by  
24 Section 5 of the FTCA, 15 U.S.C. § 45.

25 **CLASS ACTION ALLEGATIONS**

26 93. Plaintiffs sues on behalf of themselves and the proposed Class (“Class”), defined as  
27 follows: “All individuals residing in the United States whose PII was compromised in the  
28 Data Breach disclosed by Ethos in December 2022.” Excluded from the Class are Defendant, its

1 agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest,  
2 any Defendant officer or director, any successor or assign, and any Judge who adjudicates this  
3 case, including their staff and immediate family.

4 94. Plaintiffs reserve the right to amend the class definition.

5 95. This action satisfies the numerosity, commonality, typicality, and adequacy  
6 requirements under Fed. R. Civ. P. 23.

- 7 a. **Numerosity**. Plaintiffs are representative of the proposed Class, consisting of  
8 thousands of members, far too many to join in a single action;
- 9 b. **Ascertainability**. Class members are readily identifiable from information in  
10 Defendant's possession, custody, and control;
- 11 c. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises  
12 from the same Data Breach, the same alleged violations by Defendant, and the  
13 same unreasonable manner of notifying individuals about the Data Breach.
- 14 d. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's  
15 interests. Their interests do not conflict with Class members' interests, and they  
16 have retained counsel experienced in complex class action litigation and data  
17 privacy to prosecute this action on the Class's behalf, including as lead counsel.
- 18 e. **Commonality**. Plaintiffs' and the Class's claims raise predominantly common  
19 fact and legal questions that a class wide proceeding can answer for all Class  
20 members. Indeed, it will be necessary to answer the following questions:
  - 21 i. Whether Defendant had a duty to use reasonable care in safeguarding  
22 Plaintiffs' and the Class's PII;
  - 23 ii. Whether Defendant failed to implement and maintain reasonable security  
24 procedures and practices appropriate to the nature and scope of the  
25 information compromised in the Data Breach;
  - 26 iii. Whether Defendant was negligent in maintaining, protecting, and securing  
27 PII;

28 ///



1 to properly supervise both the way the PII was stored, used, and exchanged, and those in its  
2 employ who were responsible for making that happen.

3 100. Defendant owed to Plaintiffs and members of the Class a duty to notify them  
4 within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a  
5 duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature,  
6 and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and  
7 members of the Class to take appropriate measures to protect their PII, to be vigilant in the face  
8 of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the  
9 Data Breach.

10 101. Defendant owed these duties to Plaintiffs and members of the Class because they  
11 are members of a well-defined, foreseeable, and probable class of individuals whom Defendant  
12 knew or should have known would suffer injury-in-fact from Defendant's inadequate security  
13 protocols. Defendant actively sought and obtained Plaintiffs' and members of the Class's  
14 personal information and PII.

15 102. The risk that unauthorized persons would attempt to gain access to the PII and  
16 misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that  
17 unauthorized individuals would attempt to access Defendant's databases containing the PII—  
18 whether by malware or otherwise.

19 103. PII is highly valuable, and Defendant knew, or should have known, the risk in  
20 obtaining, using, handling, emailing, and storing the PII of Plaintiffs and members of the Class  
21 and the importance of exercising reasonable care in handling it.

22 104. Defendant breached its duties by failing to exercise reasonable care in supervising  
23 its agents, contractors, vendors, and suppliers, and in handling and securing the personal  
24 information and PII of Plaintiffs and members of the Class which actually and proximately  
25 caused the Data Breach and Plaintiffs' and members of the Class's injury. Defendant further  
26 breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs  
27 and members of the Class, which actually and proximately caused and exacerbated the harm  
28 from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact. As a direct and

1 traceable result of Defendant’s negligence and/or negligent supervision, Plaintiffs and members  
2 of the Class have suffered or will suffer damages, including monetary damages, increased risk of  
3 future harm, embarrassment, humiliation, frustration, and emotional distress.

4 105. Defendant’s breach of its common-law duties to exercise reasonable care and its  
5 failures and negligence actually and proximately caused Plaintiffs and members of the Class  
6 actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII  
7 by criminals, improper disclosure of their PII, lost value of their PII, and lost time and money  
8 incurred to mitigate and remediate the effects of the Data Breach that resulted from and were  
9 caused by Defendant’s negligence, which injury-in-fact and damages are ongoing, imminent,  
10 immediate, and which they continue to face.

11 **COUNT II**

12 **NEGLIGENCE PER SE**

13 **(ON BEHALF OF PLAINTIFFS AND THE CLASS)**

14 106. Plaintiffs and members of the Class incorporate the above allegations as if fully  
15 set forth herein.

16 107. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and  
17 adequate computer systems and data security practices to safeguard Plaintiffs’ and members of  
18 the Class’s PII.

19 108. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting  
20 commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by  
21 businesses, such as Defendant, of failing to use reasonable measures to protect customers’ PII.  
22 The FTC publications and orders promulgated pursuant to the FTC Act also form part of the  
23 basis of Defendant’s duty to protect Plaintiffs’ and the members of the Class’s sensitive PII.

24 109. Defendant violated its duty under Section 5 of the FTC Act by failing to use  
25 reasonable measures to protect PII and not complying with applicable industry standards as  
26 described in detail herein. Defendant’s conduct was particularly unreasonable given the nature  
27 and amount of PII Defendant had collected and stored and the foreseeable consequences of a

28 ///

1 data breach, including, specifically, the immense damages that would result to individuals in the  
2 event of a breach, which ultimately came to pass.

3 110. The harm that has occurred is the type of harm the FTC Act is intended to guard  
4 against. Indeed, the FTC has pursued numerous enforcement actions against businesses that,  
5 because of their failure to employ reasonable data security measures and avoid unfair and  
6 deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the  
7 Class.

8 111. Defendant had a duty to Plaintiffs and the members of the Class to implement and  
9 maintain reasonable security procedures and practices to safeguard Plaintiffs' and the Class's  
10 PII.

11 112. Defendant breached its respective duties to Plaintiffs and members of the Class  
12 under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data  
13 security practices to safeguard Plaintiffs' and members of the Class's PII.

14 113. Defendant's violation of Section 5 of the FTC Act and its failure to comply with  
15 applicable laws and regulations constitutes negligence per se.

16 114. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs  
17 and members of the Class, Plaintiffs and members of the Class would not have been injured.

18 115. The injury and harm suffered by Plaintiffs and members of the Class were the  
19 reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should  
20 have known that Defendant was failing to meet its duties and that its breach would cause  
21 Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure  
22 of their PII.

23 116. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and  
24 members of the Class have suffered harm, including loss of time and money resolving fraudulent  
25 charges; loss of time and money obtaining protections against future identity theft; lost control  
26 over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to  
27 exceeding credit and debit card limits and balances; harm resulting from damaged credit scores

28 ///

1 and information; and other harm resulting from the unauthorized use or threat of unauthorized  
2 use of stolen personal information, entitling them to damages in an amount to be proven at trial.

3 **COUNT III**

4 **INVASION OF PRIVACY**

5 **(ON BEHALF OF PLAINTIFFS AND THE CLASS)**

6 117. Plaintiffs incorporate by reference all preceding allegations.

7 118. Under California law, a defendant is liable for invasion of privacy if: (1) the  
8 plaintiff possessed a legally protected privacy interest, (2) in which the plaintiff maintained a  
9 reasonable expectation of privacy, and (3) the defendant's intrusion into that privacy interest was  
10 highly offensive. (*See, e.g., Hernandez v. Hillsides, Inc.* (2009) Cal. 4th 272, 287.)

11 119. Defendant knew, or should have known, that its data security practices were  
12 inadequate and had numerous vulnerabilities.

13 120. Defendant recklessly or negligently failed to take reasonable precautions to ensure  
14 its data systems were protected.

15 121. Defendant knew or should have known that its acts and omissions would likely  
16 result in a data breach, which would necessarily cause harm to Plaintiffs and the Class.

17 122. The exposure of Plaintiffs' information is a highly offensive breach of social  
18 norms.

19 123. Plaintiffs and the Class had a reasonable, legally protected privacy interest in their  
20 PII.

21 124. As a result of Defendant's acts and omissions, third parties accessed the PII of  
22 Plaintiffs and the Class without authorization.

23 125. Defendant is liable to Plaintiffs and the Class for damages in an amount to be  
24 determined at trial.

25 ///

26 ///

27 ///

28 ///

**COUNT V:**

**VIOLATIONS OF THE UNFAIR COMPETITION LAW,**

**BUS. & PROF. CODE § 17200, *ET SEQ.***

**(ON BEHALF OF PLAINTIFFS AND THE CLASS)**

126. Plaintiffs incorporate by reference all preceding allegations.

127. The California Unfair Competition Law provides that:

“[U]nfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by Chapter 1 (commencing with Section 17500) of Part 3 of Division 7 of the Business and Professions Code.” (BUS. & PROF. CODE § 17200.)

128. Defendant stored the PII of Plaintiffs and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiffs’ and the Class’s PII secure and prevented the loss or misuse of that PII.

129. Defendant failed to disclose to Plaintiffs and the Class that their PII was not secure. At no time were Plaintiffs and the Class on notice that their PII was not secure, which Defendant had a duty to disclose.

130. Had Defendant complied with these requirements, Plaintiffs and the Class would not have suffered the damages related to the data breach.

131. Defendant’s conduct was unlawful, in that it violated the policy set forth in California’s Consumer Records Act, requiring the safeguard of personal information like Social Security numbers, the FTCA, as identified above, and Defendant’s common law duty to safeguard PII.

132. Defendant’s conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

133. Defendant also engaged in unfair business practices under the “tethering test.” Its actions and omissions, as described above, violated fundamental public policies expressed by the

1 California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 (“The Legislature declares that . . . all  
2 individuals have a right of privacy in information pertaining to them . . . The increasing use of  
3 computers . . . has greatly magnified the potential risk to individual privacy that can occur from  
4 the maintenance of personal information.”); Cal. Civ. Code § 1798.81.5(a) (“It is the intent of the  
5 Legislature to ensure that personal information about California residents is protected.”); Cal.  
6 Bus. & Prof. Code § 22578 (“It is the intent of the Legislature that this chapter [including the  
7 Online Privacy Protection Act] is a matter of statewide concern.”). Defendant’s acts and  
8 omissions thus amount to a violation of the law.

9 134. As a result of those unlawful and unfair business practices, Plaintiffs and the  
10 Class suffered an injury-in-fact and have lost money or property.

11 135. The injuries to Plaintiffs and the Class greatly outweigh any alleged  
12 countervailing benefit to consumers or competition under all of the circumstances.

13 136. There were reasonably available alternatives to further Defendant’s legitimate  
14 business interests, other than the misconduct alleged in this complaint.

15 137. Therefore, Plaintiffs and the Class are entitled to equitable relief, including  
16 restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to  
17 Defendant because of its unfair and improper business practices; a permanent injunction  
18 enjoining Defendant’s unlawful and unfair business activities; and any other equitable relief the  
19 Court deems proper.

20 **COUNT V**

21 **DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF**

22 **(ON BEHALF OF PLAINTIFFS AND THE CLASSES)**

23 138. Plaintiffs incorporate all previous paragraphs as if fully set forth below.

24 139. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is  
25 authorized to enter a judgment declaring the rights and legal relations of the parties and to grant  
26 further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those  
27 alleged herein, which are tortious and which violate the terms of the federal and state statutes  
28 described above.

1           140. An actual controversy has arisen in the wake of the Data Breach at issue regarding  
2 Defendant's common law and other duties to act reasonably with respect to employing  
3 reasonable data security. Plaintiffs allege Defendant's actions in this respect were inadequate and  
4 unreasonable and, upon information and belief, remain inadequate and unreasonable.  
5 Additionally, Plaintiffs and the Classes continue to suffer injury due to the continued and  
6 ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

7           141. Pursuant to its authority under the Declaratory Judgment Act, this Court should  
8 enter a judgment declaring, among other things, the following:

- 9           a. Defendant owed, and continues to owe, a legal duty to employ reasonable data  
10 security to secure the PII it possesses, and to notify impacted individuals of the  
11 Data Breach under the common law and Section 5 of the FTC Act;
- 12           b. Defendant breached, and continues to breach, its duty by failing to employ  
13 reasonable measures to secure its customers' personal and financial information;  
14 and
- 15           c. Defendant's breach of its legal duty continues to cause harm to Plaintiffs and the  
16 Classes.

17           142. The Court should also issue corresponding injunctive relief requiring Defendant  
18 to employ adequate security protocols consistent with industry standards to protect its  
19 employees' (i.e. Plaintiffs and the Classes') data.

20           143. If an injunction is not issued, Plaintiffs and the Classes will suffer irreparable  
21 injury and lack an adequate legal remedy in the event of another breach of Defendant's data  
22 systems. If another breach of Defendant's data systems occurs, Plaintiffs and the Classes will not  
23 have an adequate remedy at law because many of the resulting injuries are not readily quantified  
24 in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put,  
25 monetary damages, while warranted to compensate Plaintiffs and the Classes for their out-of-  
26 pocket and other damages that are legally quantifiable and provable, do not cover the full extent  
27 of injuries suffered by Plaintiffs and the Classes, which include monetary damages that are not  
28 legally quantifiable or provable.



**JURY DEMAND**

147. Plaintiffs demands a trial by jury on all issues so triable.

Respectfully Submitted  
ADAM J SCHWARTZ ATTORNEY AT LAW

Dated: January 6, 2023

by:  \_\_\_\_\_  
Adam J Schwartz

*Attorney for JOHN BLUMENSTOCK,  
THOMAS ROSSELLO, and JEFFREY  
BRANCH and proposed class*

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