

1 John J. Nelson (SBN 317598)  
2 **MILBERG COLEMAN BRYSON**  
3 **PHILLIPS GROSSMAN PLLC**  
4 401 W. Broadway, Suite 1760  
5 San Diego, CA 92101  
6 Tel: (858) 209-6941  
7 jnelson@milberg.com

8 *Attorney for Plaintiff*

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

12 **JOSEPHINE DIBISCEGLIA**, on behalf of  
13 herself and all others similarly situated,

14 Plaintiff,

15 vs.

16 **ETHOS TECHNOLOGIES, INC.**,

17 Defendant.

Case No.: \_\_\_\_\_

**CLASS ACTION COMPLAINT**

DEMAND FOR JURY TRIAL

18 Plaintiff Josephine Dibisceglia, individually, and on behalf of all others similarly situated,  
19 brings this Class Action Complaint (“Complaint”) against Defendant Ethos Technologies, Inc.  
20 (“Ethos” or “Defendant”), to obtain damages, restitution, and injunctive relief for the Class, as  
21 defined below, from Defendant. Plaintiff makes the following allegations on information and  
22 belief, except as to her own actions, which are made on personal knowledge, the investigation of  
23 her counsel, and the facts that are a matter of public record.

24 **NATURE OF CASE**

25 1. This class action arises out of the recent targeted cyberattack and data breach  
26 (“Data Breach”) on Ethos’s network—through its third-party integrated service provider,  
27

28 CLASS ACTION COMPLAINT

1 Guidewire—that resulted in unauthorized access to highly sensitive data.<sup>1</sup> As a result of the Data  
2 Breach, Class Members suffered ascertainable losses in the form of the benefit of their bargain,  
3 out-of-pocket expenses, the value of their time reasonably incurred to remedy or mitigate the  
4 effects of the attack, emotional distress, and the present risk of imminent harm caused by the  
5 compromise of their sensitive personal information.

6 2. The specific information compromised in the Data Breach includes personally  
7 identifiable information (“PII”), including full names and Social Security numbers.  
8

9 3. Upon information and belief, prior to and through December 2022, Defendant  
10 obtained the PII of Plaintiff and Class Members and stored that PII, unencrypted, in an Internet-  
11 accessible environment on Ethos’s network, in which unauthorized actors used an extraction tool  
12 to retrieve Social Security numbers from Ethos’s third-party integrated service provider,  
13 Guidewire.

14 4. Plaintiff’s and Class Members’ PII—which was entrusted to Defendant, its  
15 officials, and agents—was compromised and unlawfully accessed due to the Data Breach.  
16

17 5. Plaintiff brings this class action lawsuit on behalf of those similarly situated to  
18 address Defendant’s inadequate safeguarding of her and Class Members’ PII that Defendant  
19 collected and maintained, and for Defendant’s failure to provide timely and adequate notice to  
20 Plaintiff and other Class Members that their PII had been subject to the unauthorized access of  
21 an unknown, unauthorized party.  
22

23 6. Defendant maintained the PII in a negligent and/or reckless manner. In particular,  
24 the PII was maintained on Defendant’s computer system and network in a condition vulnerable  
25 to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for  
26

---

27 <sup>1</sup> <https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-21.pdf>

1 improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and  
2 thus Defendant was on notice that failing to take steps necessary to secure the PII from those risks  
3 left that property in a dangerous condition.

4 7. Upon information and belief, Defendant and its employees additionally failed to  
5 properly monitor the computer network, IT systems, and integrated service that housed Plaintiff's  
6 and Class Members' PII.

7 8. As a result of Defendant's negligent conduct, Plaintiff's and Class Members'  
8 identities are now at risk because the PII that Defendant collected and maintained is now in the  
9 hands of malicious cybercriminals. The risks to Plaintiff and Class Members will remain for their  
10 respective lifetimes.

11 9. Defendant failed to provide timely, accurate, and adequate notice to Plaintiff and  
12 Class Members. Plaintiff's and Class Members' knowledge about the PII that Defendant allowed  
13 to be compromised, as well as precisely what type of information was unencrypted and in the  
14 possession of unknown third parties, was unreasonably delayed by Defendant's failure to warn  
15 impacted persons immediately upon learning of the Data Breach.

16 10. In letters dated December 21, 2022, Ethos notified state Attorneys General and  
17 some Class Members about the widespread data breach that had occurred on Ethos's computer  
18 network and that Class Members' PII was accessed and acquired by malicious actors, using  
19 Guidewire's integrated insurance services (the "Notice").<sup>2</sup>

20 11. The Notice provided to the Montana Attorney General is as follows:

21  
22  
23 **What Happened?** Ethos offers life insurance policies through an online  
24 application process. On December 8, 2022, we learned that unauthorized  
25 actors had launched a sophisticated and successful cyberattack against our  
26 website to access certain persons' SSNs. We immediately investigated the

---

27 <sup>2</sup> *Id.*

1 incident and made a series of technical changes to our website to prevent  
2 further unauthorized access to SSNs. The vast majority of people affected  
3 by this incident were not existing Ethos customers.

4 To access SSNs, the unauthorized actors entered information they had  
5 obtained about you from other sources—first and last name, date of birth,  
6 and address—into our online insurance application flow. This caused a  
7 third-party integrated service to return your SSN to the page source code on  
8 our website. Then, the unauthorized actors used specialized tools to extract  
9 SSNs from the page source code of our website. Importantly, these SSNs  
10 did not appear on the public-facing application page of the site. The incident  
11 spanned from approximately August 4, 2022 through December 9, 2022.

12 **What Information Was Involved?** Social Security number.<sup>3</sup>

13 12. Ethos acknowledged that its investigation into the Data Breach determined there  
14 was unauthorized access to Plaintiff’s and Class Members’ Social Security numbers between  
15 August 4, 2022, and December 9, 2022. Ethos’s investigation concluded, and it learned what  
16 information was available to the unauthorized actors, on December 8, 2022.

17 13. Ethos’s Notice letter further admitted that the PII accessed included individuals’  
18 names and Social Security numbers.<sup>4</sup>

19 14. Armed with the PII accessed in the Data Breach, data thieves can commit a variety  
20 of crimes including opening new financial accounts in Class Members’ names, taking out loans  
21 in Class Members’ names, using Class Members’ names to obtain medical services, using Class  
22 Members’ information to target other phishing and hacking intrusions using Class Members’  
23 information to obtain government benefits, filing fraudulent tax returns using Class Members’  
24 information, obtaining driver’s licenses in Class Members’ names but with another person’s  
25 photograph, and giving false information to police during an arrest.

26 <sup>3</sup> *Id.*

27 <sup>4</sup> *Id.*

1 15. As a result of the Data Breach, Plaintiff and Class Members have been exposed to  
2 a present, heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members  
3 must now closely monitor their financial accounts to guard against identity theft for the rest of  
4 their lives.

5 16. Plaintiff and Class Members may also incur out of pocket costs for purchasing  
6 credit monitoring services, credit freezes, credit reports, or other protective measures to deter and  
7 detect identity theft.

8 17. By her Complaint, Plaintiff seeks to remedy these harms on behalf of herself and  
9 all similarly situated individuals whose PII was accessed during the Data Breach.

10 18. Accordingly, Plaintiff brings claims on behalf of herself and the Class for: (i)  
11 negligence, (ii) invasion of privacy, (iii) unjust enrichment and (iv) violation of the California  
12 Unfair Competition Law. Through these claims, Plaintiff seeks, *inter alia*, damages and  
13 injunctive relief, including improvements to Defendant's data security systems and integrated  
14 services, future annual audits, and adequate credit monitoring services.  
15  
16

17 **THE PARTIES**

18 19. Plaintiff Josephine Dibisceglia is a natural person, resident, and a citizen of the  
19 State of Florida. Plaintiff Dibisceglia has no intention of moving to a different state in the  
20 immediate future. Plaintiff Dibisceglia is acting on her own behalf and on behalf of others  
21 similarly situated. Defendant obtained and continues to maintain Plaintiff Dibisceglia's PII and  
22 owes her a legal duty and obligation to protect that PII from unauthorized access and disclosure.  
23 Plaintiff Dibisceglia's PII was compromised and disclosed as a result of Defendant's inadequate  
24 data security, which resulted in the Data Breach.  
25  
26  
27  
28

1 20. Plaintiff received a notice letter from Ethos, dated December 21, 2022, stating that  
2 a data security incident occurred at Ethos and Plaintiff's PII was involved in the incident.

3 21. Defendant Ethos Technologies Inc. is a provider of insurance, specializing in life  
4 insurance. Defendant is headquartered at 75 Hawthorne Street, Suite 2000, San Francisco,  
5 California 94105.

6 **JURISDICTION AND VENUE**  
7

8 22. This Court has original jurisdiction over this action under the Class Action  
9 Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, including  
10 Plaintiff, are citizens of a different state than Defendant, there are more than 100 putative class  
11 members, and the amount in controversy exceeds \$5 million exclusive of interest and costs.

12 23. This Court has personal jurisdiction over Defendant because Defendant and/or  
13 their parents or affiliates are headquartered in this District and Defendant conducts substantial  
14 business in California and this District through its headquarters, offices, parents, and affiliates.

15 24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's  
16 principal places of business are in this District and a substantial part of the events, acts, and  
17 omissions giving rise to Plaintiff's claims occurred in this District.

18 **DIVISIONAL ASSIGNMENT**  
19

20 25. This Action is properly assigned to the San Francisco Division of this District  
21 pursuant to N.D. Cal. L.R. 3-2, because Ethos maintains its principal place of business in San  
22 Francisco, which is served by the San Francisco Division of this District.

23 **DEFENDANT'S BUSINESS**  
24

25 26. Defendant Ethos is an insurance carrier, specializing in life insurance.  
26

27 CLASS ACTION COMPLAINT  
28

1           27.    Upon information and belief, in the course of its day-to-day business operations,  
2 Defendant maintains the PII of customers, insurance applicants, and others, including but not  
3 limited to:

- 4           • Name, address, phone number and email address;
- 5           • Date of birth;
- 6           • Demographic information;
- 7           • Social Security number;
- 8           • Financial information;
- 9           • Information relating to individual medical history;
- 10          • Information concerning an individual’s doctor, nurse, or other medical providers;
- 11          • Medication information,
- 12          • Health insurance information,
- 13          • Photo identification;
- 14          • Employment information, and;
- 15          • Other information that Defendant may deem necessary to provide care.

16           28.    Additionally, Defendant may receive PII from other individuals and/or  
17 organizations that are part of a customers’ “circle of care,” such as referring physicians,  
18 customers’ other doctors, customers’ health plan(s), close friends, and/or family members.  
19

20           29.    Plaintiff and Class Members directly or indirectly entrusted Defendant with  
21 sensitive and confidential PII, which includes information that is static, does not change, and can  
22 be used to commit myriad financial crimes.  
23

24           30.    Upon information and belief, Defendant promised— due to the highly sensitive,  
25 confidential nature of the information it collects—to customers that Ethos would (among other  
26

1 things) keep their PII private, comply with industry standards related to data security and PII;  
2 inform them of their legal duties and comply with all federal and state laws protecting PII; only  
3 use and release their PII for reasons that relate to medical care and treatment; and provide  
4 adequate notice if their PII is disclosed without authorization.

5 31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class  
6 Members' PII, Defendant assumed legal and equitable duties and knew or should have known  
7 that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized  
8 disclosure.  
9

10 32. Plaintiff and the Class Members value their privacy and have taken reasonable  
11 steps to maintain the confidentiality of their PII.

12 33. Plaintiff and the Class Members relied on Defendant to implement and follow  
13 adequate data security policies and protocols, to keep their PII confidential and securely  
14 maintained, to use such PII solely for business purposes, and to prevent the unauthorized  
15 disclosures of their PII.  
16

17 **THE CYBERATTACK**

18 34. On or around December 8, 2022, Ethos became aware of suspicious activity in its  
19 network environment and its website.

20 35. Defendant Ethos investigated the suspicious activity, and through its  
21 investigation, determined that its network was subject to a cyber-attack using the integrated  
22 service software on its website. Unauthorized actors exploited this integrated software to target,  
23 access, and acquire the PII without authorization.  
24  
25  
26  
27



1 36. The investigation determined that private information related to certain customers  
2 and other individuals on Ethos’s website was accessed and taken by an unauthorized user between  
3 August 4, 2022, and December 9, 2022.

4 37. As Defendant admits, Plaintiff’s and Class Members’ PII was exfiltrated and  
5 stolen in the attack.

6 38. Upon information and belief, the unauthorized actors were able to access Ethos’s  
7 insurance application flow on its website by entering certain consumer information that they had  
8 obtained through other sources. This simple maneuver prompted a return of the named  
9 consumers’ Social Security numbers in the application. The PII was internet accessible,  
10 unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized  
11 actor.  
12

13 39. It is likely the Data Breach was targeted at Defendant due to its status as an  
14 insurance related service provider that collects, creates, and maintains sensitive PII.  
15

16 40. Upon information and belief, the cyberattack was expressly designed to gain  
17 access to private and confidential data of specific individuals, including (among other things) the  
18 PII of Plaintiff and the Class Members.

19 41. Ethos admitted that the stolen information included full names and Social Security  
20 Numbers.  
21

22 42. While Ethos stated in the Notice letter that the unauthorized activity occurred and  
23 was discovered on December 8, 2022, Defendant did notify the specific persons or entities whose  
24 PII was acquired and exfiltrated until December 21, 2022—*over five months* after the Data Breach  
25 began on August 4, 2022.  
26  
27  
28

1           43.     Upon information and belief, and based on the type of cyberattack, it is plausible  
2 and likely that Plaintiff’s PII was stolen in the Data Breach. Plaintiff further believes her PII was  
3 likely subsequently sold on the dark web following the Data Breach, as that is the *modus operandi*  
4 of cybercriminals.

5           44.     Defendant had a duty to adopt reasonable measures to protect Plaintiff’s and Class  
6 Members’ PII from involuntary disclosure to third parties.

7           45.     In response to the Data Breach, Ethos admits they worked with an “independent  
8 forensic investigation firm” to determine the nature and scope of the incident and purports to have  
9 taken steps to secure the systems.

10          46.     Ethos admits additional security was required, but there is no indication whether  
11 these steps are adequate to protect Plaintiff’s and Class Members’ PII going forward.

12          47.     Because of the Data Breach, data thieves were able to gain access to Defendant’s  
13 supposedly secure systems for months (between August 4, 2022, and December 9, 2021) and  
14 were able to compromise, access, and acquire the protected PII of Plaintiff and Class Members.  
15

16          48.     Defendant had obligations created by contract, industry standards, common law,  
17 and their own promises and representations made to Plaintiff and Class Members to keep their  
18 PII confidential and to protect them from unauthorized access and disclosure.

19          49.     Plaintiff and the Class Members reasonably relied (directly or indirectly) on this  
20 sophisticated party to keep their sensitive PII confidential; to maintain proper system security; to  
21 use this information for business purposes only; and to make only authorized disclosures of their  
22 PII.  
23

24          50.     Plaintiff’s and Class Members’ unencrypted, unredacted PII was compromised  
25 due to Defendant’s negligent and/or careless acts and omissions, and due to the utter failure to  
26

1 protect Class Members' PII. Criminal hackers obtained their PII because of its value in exploiting  
2 and stealing the identities of Plaintiff and Class Members. The risks to Plaintiff and Class  
3 Members will remain for their respective lifetimes.

4 **The Data Breach was a Foreseeable Risk of which Defendant was on Notice**

5 51. Defendant's data security obligations were particularly important given the  
6 substantial increase in cyberattacks and/or data breaches in the insurance industry and other  
7 industries holding significant amounts of PII preceding the date of the breach.  
8

9 52. In 2021, a record 1,862 data breaches occurred, resulting in approximately  
10 293,927,708 sensitive records being exposed, a 68% increase from 2020.<sup>5</sup> The 330 reported  
11 breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to  
12 only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.<sup>6</sup>

13 53. In light of recent high profile data breaches at other insurance partner and provider  
14 companies, Defendant knew or should have known that their electronic records and PII they  
15 maintained would be targeted by cybercriminals and ransomware attack groups.<sup>7</sup>  
16

17 54. Moreover, Ethos knew or should have known that these attacks were common and  
18 foreseeable, as it discovered a separate and distinct but substantially similar data breach in  
19 January 2022, which also occurred for approximately several months.<sup>8</sup>  
20  
21  
22

23  
24 <sup>5</sup> See 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at  
<https://notified.idtheftcenter.org/s/>), at 6.

25 <sup>6</sup> *Id.*

26 <sup>7</sup> <https://www.databreaches.net/rxamerica-and-accendo-insurance-notify-175000-medicare-beneficiaries-that-mailing-error-exposed-their-medication-name-date-of-birth-and-member-id/>

27 <sup>8</sup> <https://www.doj.nh.gov/consumer/security-breaches/documents/ethos-technologies-20220218.pdf>

1 55. In light of recent high profile cybersecurity incidents at other insurance partners and  
2 provider companies, Ethos knew or should have known that their electronic records would be  
3 targeted by cybercriminals.<sup>9</sup>

4 56. Therefore, the increase in such attacks, and attendant risk of future attacks, was  
5 widely known to the public and to anyone in Defendant's industry, including Ethos.

6 **Defendant Fails to Comply with FTC Guidelines**

7 57. The Federal Trade Commission ("FTC") has promulgated numerous guides for  
8 businesses which highlight the importance of implementing reasonable data security practices.  
9 According to the FTC, the need for data security should be factored into all business decision-  
10 making.  
11

12 58. In 2016, the FTC updated its publication, *Protecting Personal Information: A*  
13 *Guide for Business*, which established cyber-security guidelines for businesses. The guidelines  
14 note that businesses should protect the personal customer information that they keep; properly  
15 dispose of personal information that is no longer needed; encrypt information stored on computer  
16 networks; understand its network's vulnerabilities; and implement policies to correct any security  
17 problems.<sup>10</sup> The guidelines also recommend that businesses use an intrusion detection system to  
18 expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone  
19 is attempting to hack the system; watch for large amounts of data being transmitted from the  
20 system; and have a response plan ready in the event of a breach.<sup>11</sup>  
21  
22  
23

24 <sup>9</sup> <https://www.databreaches.net/rxamerica-and-accendo-insurance-notify-175000-medicare-beneficiaries-that-mailing-error-exposed-their-medication-name-date-of-birth-and-member-id/>

25 <sup>10</sup> *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).  
26 Available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited Jan. 19, 2022).

27 <sup>11</sup> *Id.*

1 59. The FTC further recommends that companies not maintain PII longer than is  
2 needed for authorization of a transaction; limit access to sensitive data; require complex  
3 passwords to be used on networks; use industry-tested methods for security; monitor for  
4 suspicious activity on the network; and verify that third-party service providers have  
5 implemented reasonable security measures.

6 60. The FTC has brought enforcement actions against businesses for failing to  
7 adequately and reasonably protect customer data, treating the failure to employ reasonable and  
8 appropriate measures to protect against unauthorized access to confidential consumer data as an  
9 unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”),  
10 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must  
11 take to meet their data security obligations.  
12

13 61. These FTC enforcement actions include actions against insurance providers and  
14 partners like Defendant.  
15

16 62. Defendant failed to properly implement basic data security practices.

17 63. Defendant’s failure to employ reasonable and appropriate measures to protect  
18 against unauthorized access to customers and other impacted individuals’ PII constitutes an unfair  
19 act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.  
20

21 64. Defendant was at all times fully aware of their obligation to protect the PII.  
22 Defendant was also aware of the significant repercussions that would result from their failure to  
23 do so.  
24  
25  
26  
27  
28

**Defendant Fails to Comply with Industry Standards**

1  
2 65. As shown above, experts studying cyber security routinely identify insurance  
3 providers and partners as being particularly vulnerable to cyberattacks because of the value of  
4 the PII which they collect and maintain.

5 66. Several best practices have been identified that at a minimum should be  
6 implemented by insurance providers, like Defendant, including but not limited to: educating all  
7 employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-  
8 malware software; encryption, making data unreadable without a key; multi-factor  
9 authentication; backup data; and limiting which employees can access sensitive data.  
10

11 67. Other best cybersecurity practices that are standard in the insurance industry  
12 include installing appropriate malware detection software; monitoring and limiting the network  
13 ports; protecting web browsers and email management systems; setting up network systems such  
14 as firewalls, switches and routers; monitoring and protection of physical security systems;  
15 protection against any possible communication system; training staff regarding critical points.  
16

17 68. Defendant failed to meet the minimum standards of any of the following  
18 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation  
19 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,  
20 PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center  
21 for Internet Security’s Critical Security Controls (CIS CSC), which are all established standards  
22 in reasonable cybersecurity readiness.  
23

24 69. These foregoing frameworks are existing and applicable industry standards in the  
25 insurance industry, and Defendant failed to comply with these accepted standards, thereby  
26 opening the door to the cyber incident and causing the data breach.  
27

**DEFENDANT’S BREACH**

1  
2 70. Defendant breached its obligations to Plaintiff and Class Members and/or were  
3 otherwise negligent and reckless because Ethos failed to properly maintain and safeguard their  
4 computer systems and website’s application flow. Defendant’s unlawful conduct includes, but is  
5 not limited to, the following acts and/or omissions:

- 6 a. Failing to maintain an adequate data security system to reduce the risk of  
7 data breaches and cyber-attacks;
- 8 b. Failing to adequately protect PII;
- 9 c. Failing to properly monitor their own data security systems for existing  
10 intrusions;
- 11 d. Failing to ensure that their vendors with access to their computer systems  
12 and data employed reasonable security procedures;
- 13 e. Failing to ensure the confidentiality and integrity of electronic PII it  
14 created, received, maintained, and/or transmitted;
- 15 f. Failing to implement technical policies and procedures for electronic  
16 information systems that maintain electronic PII to allow access only to  
17 those persons or software programs that have been granted access rights;
- 18 g. Failing to implement policies and procedures to prevent, detect, contain,  
19 and correct security violations;
- 20 h. Failing to implement procedures to review records of information system  
21 activity regularly, such as audit logs, access reports, and security incident  
22 tracking reports;
- 23
- 24
- 25
- 26
- 27
- 28

- i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PII;
- j. Failing to train all members of their workforces effectively on the policies and procedures regarding PII;
- k. Failing to render the electronic PII it maintained unusable, unreadable, or indecipherable to unauthorized individuals;
- l. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;
- m. Failing to adhere to industry standards for cybersecurity as discussed above; and,
- n. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' PII.

71. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access Defendant's online insurance application flow, which provided unauthorized actors with unsecured and unencrypted PII.

72. Accordingly, as outlined below, Plaintiff and Class Members now face a present, increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members lost the benefit of the bargain they made with Defendant.

**Data Breaches Cause Disruption and Increased Risk of Fraud and Identity Theft**

73. Cyberattacks and data breaches at insurance companies and insurance software companies, like Defendant, are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.



1           74.     The United States Government Accountability Office released a report in 2007  
2 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face  
3 “substantial costs and time to repair the damage to their good name and credit record.”<sup>12</sup>

4           75.     That is because any victim of a data breach is exposed to serious ramifications  
5 regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable  
6 information is to monetize it. They do this by selling the spoils of their cyberattacks on the black  
7 market to identity thieves who desire to extort and harass victims, take over victims’ identities in  
8 order to engage in illegal financial transactions under the victims’ names. Because a person’s  
9 identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a  
10 person, the easier it is for the thief to take on the victim’s identity, or otherwise harass or track  
11 the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking  
12 technique referred to as “social engineering” to obtain even more information about a victim’s  
13 identity, such as a person’s login credentials or Social Security number. Social engineering is a  
14 form of hacking whereby a data thief uses previously acquired information to manipulate  
15 individuals into disclosing additional confidential or personal information through means such as  
16 spam phone calls and text messages or phishing emails.  
17

18           76.     The FTC recommends that identity theft victims take several steps to protect their  
19 personal and financial information after a data breach, including contacting one of the credit  
20 bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone  
21 steals their identity), reviewing their credit reports, contacting companies to remove fraudulent  
22  
23  
24

25  
26 \_\_\_\_\_  
27 <sup>12</sup> See U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are  
28 Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is  
Unknown (2007). Available at <https://www.gao.gov/new.items/d07737.pdf>.

1 charges from their accounts, placing a credit freeze on their credit, and correcting their credit  
2 reports.<sup>13</sup>

3 77. Identity thieves use stolen personal information such as Social Security numbers  
4 for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance  
5 fraud.

6 78. Identity thieves can also use Social Security numbers to obtain a driver's license  
7 or official identification card in the victim's name but with the thief's picture; use the victim's  
8 name and Social Security number to obtain government benefits; or file a fraudulent tax return  
9 using the victim's information. In addition, identity thieves may obtain a job using the victim's  
10 Social Security number, rent a house or receive medical services in the victim's name, and may  
11 even give the victim's personal information to police during an arrest resulting in an arrest  
12 warrant being issued in the victim's name.

14 79. Moreover, theft of PII is also gravely serious because PII is an extremely valuable  
15 property right.<sup>14</sup>

17 80. Its value is axiomatic, considering the value of "big data" in corporate America  
18 and the fact that the consequences of cyber thefts include heavy prison sentences. Even this  
19 obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

---

24 <sup>13</sup> See *IdentityTheft.gov*, Federal Trade Commission, <https://www.identitytheft.gov/Steps> (last  
25 visited Jan. 19, 2022).

26 <sup>14</sup> See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable  
27 Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at \*3-4  
(2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching  
28 a level comparable to the value of traditional financial assets.") (citations omitted).

1 81. It must also be noted there may be a substantial time lag – measured in years --  
2 between when harm occurs and when it is discovered, and also between when PII is stolen and  
3 when it is used.

4 82. According to the U.S. Government Accountability Office, which conducted a  
5 study regarding data breaches:

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

12 83. PII is such a valuable commodity to identity thieves that once the information has  
13 been compromised, criminals often trade the information on the “cyber black-market” for years.

14 84. There is a strong probability that entire batches of stolen information have been  
15 dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and  
16 Class Members are at an increased risk of fraud and identity theft for many years into the future.

17 85. Thus, Plaintiff and Class Members must vigilantly monitor their financial and  
18 medical accounts for many years to come.

19 86. PII can sell for as much as \$363 per record according to the Infosec Institute.<sup>16</sup> PII  
20 is particularly valuable because criminals can use it to target victims with frauds and scams. Once  
21 PII is stolen, fraudulent use of that information and damage to victims may continue for years.

22  
23  
24  
25 <sup>15</sup> GAO Report, at p. 29.

26 <sup>16</sup> See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015),  
27 [https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-](https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/)  
28 [market/](https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/).

1           87. For example, the Social Security Administration has warned that identity thieves  
2 can use an individual's Social Security number to apply for additional credit lines.<sup>17</sup> Such fraud  
3 may go undetected until debt collection calls commence months, or even years, later. Stolen  
4 Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for  
5 unemployment benefits, or apply for a job using a false identity.<sup>18</sup> Each of these fraudulent  
6 activities is difficult to detect. An individual may not know that his or her Social Security Number  
7 was used to file for unemployment benefits until law enforcement notifies the individual's  
8 employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an  
9 individual's authentic tax return is rejected.  
10

11           88. Moreover, it is not an easy task to change or cancel a stolen Social Security  
12 number.

13           89. An individual cannot obtain a new Social Security number without significant  
14 paperwork and evidence of actual misuse. Even then, a new Social Security number may not be  
15 effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the  
16 old number, so all of that old bad information is quickly inherited into the new Social Security  
17 number.”<sup>19</sup>  
18

19           90. This data, as one would expect, demands a much higher price on the black market.  
20 Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit  
21

---

22  
23  
24 <sup>17</sup> *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1.  
25 Available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (Jan. 19, 2022).

26 <sup>18</sup> *Id* at 4.

27 <sup>19</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>.

1 card information, personally identifiable information and Social Security numbers are worth  
2 more than 10x on the black market.”<sup>20</sup>

3 91. Because of the value of its collected and stored data, the insurance industry has  
4 experienced disproportionately higher numbers of data theft events than other industries.

5 92. For this reason, Defendant knew or should have known about these dangers and  
6 strengthened its data and email handling systems accordingly. Defendant was put on notice of the  
7 substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly  
8 prepare for that risk.

9  
10 **Plaintiff’s and Class Members’ Damages**

11 93. To date, Defendant has done nothing to provide Plaintiff and the Class Members  
12 with meaningful relief for the damages they have suffered as a result of the Data Breach.

13 94. Defendant has merely offered Plaintiff and Class Members complimentary fraud  
14 and identity monitoring services for up to two years, but this does nothing to compensate them  
15 for damages incurred, time spent dealing with the Data Breach, and future fraud and identity  
16 monitoring services (reasonable and necessary expenses) beyond the two years offered.

17 95. Plaintiff and Class Members have been damaged by the compromise of their PII  
18 in the Data Breach.

19 96. Plaintiff’s and Class Members’ full names and Social Security numbers were  
20 compromised in the Data Breach and are now in the hands of the cybercriminals who accessed  
21 Defendant’s software maintaining PII. As Ethos admits, these impacted persons were specifically  
22  
23

24  
25  
26 <sup>20</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*  
27 *Numbers*, Computer World (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

1 targeted: the cybercriminals used their names, dates of birth and addresses to steal Plaintiff's and  
2 Class Members' Social Security numbers.

3 97. Since being notified of the Data Breach, Plaintiff has significant time dealing with  
4 the impact of the Data Breach—valuable time Plaintiff otherwise would have spent on other  
5 activities, including but not limited to work and/or recreation.

6 98. Due to the Data Breach, Plaintiff anticipates spending considerable time and  
7 money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This  
8 includes changing passwords, resecuring her own computer system, cancelling fraudulent credit  
9 and debit cards opened in her name, and monitoring her financial accounts for fraudulent activity.

10 99. Plaintiff's PII was compromised as a direct and proximate result of the Data  
11 Breach.

12 100. As a direct and proximate result of Defendant's conduct, Plaintiff and Class  
13 Members have been placed at a present, imminent, immediate, and continuing risk of harm from  
14 fraud and identity theft.

15 101. As a direct and proximate result of Defendant's conduct, Plaintiff and Class  
16 Members have been forced to expend time dealing with the effects of the Data Breach.

17 102. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses  
18 such as loans opened in their names, medical services billed in their names, tax return fraud,  
19 utility bills opened in their names, credit card fraud, and similar identity theft.

20 103. Plaintiff and Class Members face substantial risk of being targeted for future  
21 phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could  
22 use that information to more effectively target such schemes to Plaintiff and Class Members.  
23 Plaintiff has already experienced fraudulent conduct, as over seven thousand dollars in fraudulent  
24  
25  
26

1 charges were placed upon her credit card and identity thieves have attempted to open new credit  
2 cards falsely under her name.

3 104. Plaintiff and Class Members may also incur out-of-pocket costs for protective  
4 measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs  
5 directly or indirectly related to the Data Breach.

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

9 106. Plaintiff and Class Members were also damaged via benefit-of-the-bargain  
10 damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied  
11 by adequate data security that complied with industry standards but was not. Part of the price  
12 Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund  
13 adequate security of Defendant's systems and Plaintiff's and Class Members' PII. Thus, the  
14 Plaintiff and the Class Members did not get what they paid for and agreed to.

15 107. Plaintiff and Class Members have spent and will continue to spend significant  
16 amounts of time to monitor their financial accounts and sensitive information for misuse.

17 108. Plaintiff and Class Members have suffered or will suffer actual injury as a direct  
18 result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket  
19 expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the  
20 Data Breach relating to:

- 21
- 22 a. Reviewing and monitoring sensitive accounts and finding fraudulent
  - 23 insurance claims, loans, and/or government benefits claims;
  - 24 b. Purchasing credit monitoring and identity theft prevention;
  - 25
  - 26
  - 27

- 1 c. Spending time on the phone with or at financial institutions, healthcare
- 2 providers, and/or government agencies to dispute unauthorized and
- 3 fraudulent activity in their name;
- 4 d. Contacting financial institutions and closing or modifying financial
- 5 accounts; and
- 6 e. Closely reviewing and monitoring Social Security Number, medical
- 7 insurance accounts, bank accounts, and credit reports for unauthorized
- 8 activity for years to come.
- 9

10 109. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII,  
11 which is believed to remain in the possession of Defendant, is protected from further breaches by  
12 the implementation of adequate security measures and safeguards, including but not limited to,  
13 making sure that the storage of data or documents containing PII is not accessible online and that  
14 access to such data is password protected.

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

18 111. As a direct and proximate result of Defendant's actions and inactions, Plaintiff  
19 and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an  
20 increased risk of future harm.

21  
22 **Plaintiff Dibisceglia's Experience**

23 112. Plaintiff Josephine Dibisceglia does not know how Defendant obtained her PII,  
24 and she had never heard of Defendant until she received the notice letter regarding the Data  
25 Breach in December 2022.



1 113. Plaintiff Dibisceglia is very careful about sharing her sensitive Private  
2 Information. Plaintiff Dibisceglia has never knowingly transmitted unencrypted sensitive PII over  
3 the internet or any other unsecured source.

4 114. Plaintiff Dibisceglia first learned of the Data Breach after receiving a data breach  
5 notification letter from Ethos, dated December 21, 2022, notifying her that Defendant suffered a  
6 data breach five months earlier and that her PII had been improperly accessed and/or obtained by  
7 unauthorized third parties while in possession of Defendant.  
8

9 115. The data breach notification letter indicated that the PII involved in the Data  
10 Breach may have included Plaintiff Dibisceglia's full name and Social Security number.

11 116. As a result of the Data Breach, Plaintiff Dibisceglia made reasonable efforts to  
12 mitigate the impact of the Data Breach after receiving the data breach notification letter, including  
13 but not limited to researching the Data Breach; contacting her bank regarding fraudulent activity;  
14 contacting credit bureaus regarding fraudulent activity; and reviewing credit reports and financial  
15 account statements for any indications of actual or attempted identity theft or fraud.  
16

17 117. Plaintiff Dibisceglia experienced actual identify theft and fraud, including over  
18 seven thousand dollars of fraudulent charges being placed on her credit card as well as the identity  
19 thieves attempting to open additional credit cards falsely under her name. Plaintiff Dibisceglia  
20 has taken significant efforts to remedy her credit file as a result of the Data Breach.

21 118. Plaintiff Dibisceglia has spent several hours and will continue to spend valuable  
22 time for the remainder of her life, that she otherwise would have spent on other activities,  
23 including but not limited to work and/or recreation.  
24

25 119. Plaintiff Dibisceglia suffered actual injury from having her PII compromised as a  
26 result of the Data Breach including, but not limited to (a) damage to and diminution in the value  
27

1 of her PII, a form of property that Defendant maintained belonging to Plaintiff Dibisceglia; (b)  
2 violation of her privacy rights; (c) the theft of her PII; and (d) present, imminent and impending  
3 injury arising from the increased risk of identity theft and fraud.

4 120. As a result of the Data Breach, Plaintiff Dibisceglia has also suffered emotional  
5 distress as a result of the release of her PII, which she believed would be protected from  
6 unauthorized access and disclosure, including anxiety about unauthorized parties viewing,  
7 selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff Dibisceglia is very  
8 concerned about identity theft and fraud, as well as the consequences of such identity theft and  
9 fraud resulting from the Data Breach.  
10

11 121. As a result of the Data Breach, Plaintiff Dibisceglia anticipates spending  
12 considerable time and money on an ongoing basis to try to mitigate and address harms caused by  
13 the Data Breach.  
14

### 15 CLASS ACTION ALLEGATIONS

16 122. Plaintiff brings this action on behalf of herself and on behalf of all other persons  
17 similarly situated (“the Class”).

18 123. Plaintiff proposes the following Class definitions, subject to amendment as  
19 appropriate:

20 **All persons identified by Defendant (or their agents or affiliates) as**  
21 **being among those individuals impacted by the Data Breach,**  
22 **including all who were sent a notice of the Data Breach (the “Class”).**

23 124. Excluded from the Class are Defendant’s officers, directors, and employees; any  
24 entity in which Defendant have a controlling interest; and the affiliates, legal representatives,  
25 attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members  
26 of the judiciary to whom this case is assigned, their families and members of their staff.  
27

1           125. Plaintiff reserves the right to amend or modify the Class and/or Subclass  
2 definitions as this case progresses.

3           126. Numerosity. The Members of the Class are so numerous that joinder of all of them  
4 is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time,  
5 based on information and belief, the Class consists of thousands of individuals whose sensitive  
6 data was compromised in the Data Breach.

7           127. Commonality. There are questions of law and fact common to the Class, which  
8 predominate over any questions affecting only individual Class Members. These common  
9 questions of law and fact include, without limitation:  
10

- 11           a. Whether Defendant unlawfully used, maintained, lost, or disclosed  
12           Plaintiff's and Class Members' PII;
- 13           b. Whether Defendant failed to implement and maintain reasonable security  
14           procedures and practices appropriate to the nature and scope of the  
15           information compromised in the Data Breach;
- 16           c. Whether Defendant's data security systems prior to and during the Data  
17           Breach complied with applicable data security laws and regulations;
- 18           d. Whether Defendant's data security systems prior to and during the Data  
19           Breach were consistent with industry standards;
- 20           e. Whether Defendant owed a duty to Class Members to safeguard their PII;
- 21           f. Whether Defendant breached its duty to Class Members to safeguard their  
22           PII;
- 23           g. Whether Defendant knew or should have known that its data security  
24           systems and monitoring processes were deficient;
- 25
- 26
- 27
- 28

- 1 h. Whether Defendant should have discovered the Data Breach sooner;
- 2 i. Whether Plaintiff and Class Members suffered legally cognizable damages
- 3 as a result of Defendant's misconduct;
- 4 j. Whether Defendant's conduct was negligent;
- 5 k. Whether Defendant breached implied contracts made with Plaintiff and
- 6 Class Members;
- 7 l. Whether Defendant was unjustly enriched by unlawfully retaining a
- 8 benefit conferred upon them by Plaintiff and Class Members;
- 9 m. Whether Defendant failed to provide notice of the Data Breach in a timely
- 10 manner; and,
- 11 n. Whether Plaintiff and Class Members are entitled to damages, civil
- 12 penalties, punitive damages, treble damages, and/or injunctive relief.
- 13

14 128. Typicality. Plaintiff's claims are typical of those of other Class Members because  
15 Plaintiff's information, like that of every other Class Member, was compromised in the Data  
16 Breach.

17 129. Adequacy of Representation. Plaintiff will fairly and adequately represent and  
18 protect the interests of the Members of the Class. Plaintiff's Counsel are competent and  
19 experienced in litigating class actions.

20 130. Predominance. Defendant has engaged in a common course of conduct toward  
21 Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the  
22 same computer system and unlawfully accessed in the same way. The common issues arising  
23 from Defendant's conduct affecting Class Members set out above predominate over any  
24  
25  
26  
27

1 individualized issues. Adjudication of these common issues in a single action has important and  
2 desirable advantages of judicial economy.

3 131. Superiority. A class action is superior to other available methods for the fair and  
4 efficient adjudication of the controversy. Class treatment of common questions of law and fact is  
5 superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class  
6 Members would likely find that the cost of litigating their individual claims is prohibitively high  
7 and would therefore have no effective remedy. The prosecution of separate actions by individual  
8 Class Members would create a risk of inconsistent or varying adjudications with respect to  
9 individual Class Members, which would establish incompatible standards of conduct for  
10 Defendant. In contrast, the conduct of this action as a Class action presents far fewer management  
11 difficulties, conserves judicial resources and the parties' resources, and protects the rights of each  
12 Class Member.  
13

14 132. Defendant has acted on grounds that apply generally to the Class as a whole, so  
15 that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on  
16 a Class-wide basis.  
17

18 133. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification  
19 because such claims present only particular, common issues, the resolution of which would  
20 advance the disposition of this matter and the parties' interests therein. Such particular issues  
21 include, but are not limited to:

- 22 a. Whether Defendant failed to timely notify the public of the Data Breach;
- 23 b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise  
24 due care in collecting, storing, and safeguarding their PII;  
25

- 1 c. Whether Defendant’s security measures to protect their data systems were  
2 reasonable in light of best practices recommended by data security experts;
- 3 d. Whether Defendant’s failure to institute adequate protective security  
4 measures amounted to negligence;
- 5 e. Whether Defendant failed to take commercially reasonable steps to  
6 safeguard consumer PII; and,
- 7  
8 f. Whether adherence to FTC data security recommendations, and measures  
9 recommended by data security experts would have reasonably prevented  
10 the Data Breach.

11 134. Finally, all members of the proposed Class are readily ascertainable. Defendant  
12 has access to Class Members' names and addresses affected by the Data Breach. Class Members  
13 have already been preliminarily identified and sent notice of the Data Breach by Defendant.

14 **CAUSES OF ACTION**

15 **FIRST COUNT**

16 **Negligence**

17 **(On Behalf of Plaintiff and the Class)**

18 135. Plaintiff re-alleges and incorporates by reference by reference herein all of the  
19 allegations contained in the preceding paragraphs.

20 136. Plaintiff and the Class entrusted Defendant with their PII on the premise and with  
21 the understanding that Defendant would safeguard their information, use their PII for business  
22 purposes only, and/or not disclose their PII to unauthorized third parties.

23  
24 137. Defendant had full knowledge of the sensitivity of the PII and the types of harm  
25 that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

1           138. By collecting and storing this data on Ethos’ computer system and network, and  
2 sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable  
3 means to secure and safeguard their computer system—and Class Members’ PII held within it—  
4 to prevent disclosure of the information, and to safeguard the information from theft. Defendant’s  
5 duty included a responsibility to implement processes by which it could detect a breach of their  
6 security systems in a reasonably expeditious period of time and to give prompt notice to those  
7 affected in the case of a data breach.  
8

9           139. Defendant owed a duty of care to Plaintiff and Class Members to provide data  
10 security consistent with industry standards and other requirements discussed herein, and to ensure  
11 that their systems and networks, and the personnel responsible for them, adequately protected the  
12 PII.

13           140. Defendant’s duty of care to use reasonable security measures arose as a result of  
14 the special relationship that existed between Defendant and the individuals who entrusted them  
15 with PII, which is recognized by laws and regulations, as well as common law. Defendant was in  
16 a superior position to ensure that their systems were sufficient to protect against the foreseeable  
17 risk of harm to Class Members from a data breach.  
18

19           141. Defendant’s duty to use reasonable security measures required Defendant to  
20 reasonably protect confidential data from any intentional or unintentional use or disclosure.

21           142. In addition, Defendant had a duty to employ reasonable security measures under  
22 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . .  
23 practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair  
24 practice of failing to use reasonable measures to protect confidential data.  
25  
26  
27

1 143. Defendant’s duty to use reasonable care in protecting confidential data arose not  
2 only as a result of the statutes and regulations described above, but also because Defendant are  
3 bound by industry standards to protect confidential PII.

4 144. Defendant breached its duties, and thus was negligent, by failing to use reasonable  
5 measures to protect Class Members’ PII. The specific negligent acts and omissions committed by  
6 Defendant include, but are not limited to, the following:

- 7 a. Failing to adopt, implement, and maintain adequate security measures to
- 8 safeguard Class Members’ PII;
- 9
- 10 b. Failing to adequately monitor the security of their networks and systems;
- 11
- 12 d. Failing to have in place mitigation policies and procedures;
- 13
- 14 e. Allowing unauthorized access to Class Members’ PII;
- 15
- 16 f. Failing to detect in a timely manner that Class Members’ PII had been
- 17
- 18 g. Failing to timely notify Class Members about the Data Breach so that they  
could take appropriate steps to mitigate the potential for identity theft and  
other damages.

19 145. Defendant owed to Plaintiff and Class Members a duty to notify them within a  
20 reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to  
21 timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence  
22 of the data breach. This duty is required and necessary for Plaintiff and Class Members to take  
23 appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm,  
24 and to take other necessary steps to mitigate the harm caused by the data breach.



1 146. Plaintiff and Class Members are also entitled to injunctive relief requiring  
2 Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit  
3 to future annual audits of those systems and monitoring procedures; and (iii) continue to provide  
4 adequate credit monitoring to all Class Members.

5 147. Defendant breached its duties to Plaintiff and Class Members by failing to provide  
6 fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's  
7 and Class Members' PII.  
8

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

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

18 150. PII is highly valuable, and Defendant knew, or should have known, the risk in  
19 obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members and the  
20 importance of exercising reasonable care in handling it.

21 151. Defendant breached its duties by failing to exercise reasonable care in supervising  
22 its agents, contractors, vendors, and suppliers, and in handling and securing the PII of  
23 Plaintiff and Class Members—which actually and proximately caused the Data Breach and  
24 injured Plaintiff and Class Members.  
25  
26  
27  
28

1 152. Defendant further breached its duties by failing to provide reasonably timely notice  
2 of the data breach to Plaintiff and Class Members, which actually and proximately caused and  
3 exacerbated the harm from the data breach and Plaintiff and Class Members' injuries-in-fact. As  
4 a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and  
5 Class Members have suffered and/or will suffer damages, including monetary damages, increased  
6 risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

7  
8 153. Defendant's breach of its common-law duties to exercise reasonable care and  
9 their failures and negligence actually and proximately caused Plaintiff and Class Members  
10 actual, tangible, injury-in-fact and damages, including, without limitation, fraudulent credit  
11 card charges, financial accounts being opened falsely in their name, the theft of their PII by  
12 criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII,  
13 and lost time and money incurred to mitigate and remediate the effects of the data breach that  
14 resulted from and were caused by Defendant's negligence, which injury-in-fact and damages  
15 are ongoing, imminent, immediate, and which they continue to face.  
16

17 **SECOND COUNT**  
18 **Invasion of Privacy**  
**(On behalf of the Plaintiff and the Class)**

19 154. Plaintiff re-alleges and incorporates by reference herein all of the  
20 allegations contained in the preceding paragraphs and brings this claim under the common law  
21 and Art. I § I of the California Constitution.

22  
23 155. Plaintiff and Class Members had a legitimate expectation of privacy regarding  
24 their PII and were accordingly entitled to the protection of this information against disclosure to  
25 unauthorized third parties.  
26

1 156. Defendant owed a duty to Plaintiff and Class Member to keep their PII  
2 confidential.

3 157. The unauthorized disclosure and/or acquisition (*i.e.*, theft) by a third party of  
4 Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

5 158. Defendant's reckless and negligent failure to protect Plaintiff's and Class  
6 Members' PII constitutes an intentional interference with Plaintiff's and the Class Members'  
7 interest in solitude or seclusion, either as to their person or as to their private affairs or concerns,  
8 of a kind that would be highly offensive to a reasonable person.

9 159. Defendant's failure to protect Plaintiff's and Class Members' PII acted with a  
10 knowing state of mind when it permitted the Data Breach because it knew its information security  
11 practices were inadequate.

12 160. Defendant knowingly did not notify Plaintiff and Class Members in a timely  
13 fashion about the Data Breach.

14 161. Because Defendant failed to properly safeguard Plaintiff's and Class Members'  
15 PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury  
16 to Plaintiff and the Class.

17 162. As a proximate result of Defendant's acts and omissions, the private and sensitive  
18 PII of Plaintiff and the Class Members was stolen by a third party and is now available for  
19 disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer  
20 damages.

21 163. Defendant's wrongful conduct will continue to cause great and irreparable injury  
22 to Plaintiff and the Class since their PII is still maintained by Defendant with their inadequate  
23 cybersecurity system and policies.

1 164. Plaintiff and Class Members have no adequate remedy at law for the injuries  
2 relating to Defendant's continued possession of their sensitive and confidential records. A  
3 judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff  
4 and the Class.

5 165. Plaintiff, on behalf of herself and Class Members, seeks injunctive relief to enjoin  
6 Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class  
7 Members' PII.

8 166. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages  
9 for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by  
10 Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus  
11 prejudgment interest, and costs.  
12

13 **THIRD COUNT**  
14 **Unjust Enrichment**  
15 **(On Behalf of Plaintiff and the Class)**

16 167. Plaintiff re-alleges and incorporates by reference by reference herein all of the  
17 allegations contained in the preceding paragraphs.

18 168. Upon information and belief, Defendant funds its data security measures entirely  
19 from their general revenue, including payments made by or on behalf of Plaintiff and the Class  
20 Members.

21 169. As such, a portion of the payments made by or on behalf of Plaintiff and the Class  
22 Members is to be used to provide a reasonable level of data security, and the amount of the portion  
23 of each payment made that is allocated to data security is known to Defendant.  
24

25 170. Plaintiff and Class Members conferred a monetary benefit upon Defendant.  
26 Specifically, they purchased goods and services from Defendant and/or their agents and in so  
27

1 doing provided Defendant with their PII. In exchange, Plaintiff and Class Members should have  
2 received from Defendant the goods and services that were the subject of the transaction and have  
3 their PII protected with adequate data security.

4 171. Plaintiff and Class Members conferred a monetary benefit on Defendant, by  
5 paying Defendant as part of Defendant rendering insurance related services, a portion of which  
6 was to have been used for data security measures to secure Plaintiff's and Class Members' PII,  
7 and by providing Defendant with their valuable PII.  
8

9 172. Defendant knew that Plaintiff and Class Members conferred a benefit which  
10 Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and  
11 Class Members for business purposes.

12 173. Defendant was enriched by saving the costs they reasonably should have expended  
13 on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a  
14 reasonable level of security that would have prevented the Data Breach, Defendant instead  
15 calculated to avoid the data security obligations at the expense of Plaintiff and Class Members  
16 by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other  
17 hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite  
18 security.  
19

20 174. Under the principles of equity and good conscience, Defendant should not be  
21 permitted to retain the money belonging to Plaintiff and Class Members, because Defendant  
22 failed to implement appropriate data management and security measures that are mandated by  
23 industry standards.  
24

25 175. Defendant acquired the monetary benefit and PII through inequitable means in  
26 that it failed to disclose the inadequate security practices previously alleged.  
27

1 176. If Plaintiff and Class Members knew that Defendant had not secured their PII, they  
2 would not have agreed to provide their PII to Defendant.

3 177. Plaintiff and Class Members have no adequate remedy at law.

4 178. As a direct and proximate result of Defendant's conduct, Plaintiff and Class  
5 Members have suffered and will suffer injury including, without limitation, fraudulent credit  
6 card charges, financial accounts being opened falsely in their name, the theft of their PII by  
7 criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII,  
8 and lost time and money incurred to mitigate and remediate the effects of the data breach that  
9 resulted from and were caused by Defendant's misconduct, which injury-in-fact and damages  
10 are ongoing, imminent, immediate, and which they continue to face.

12 179. As a direct and proximate result of Defendant's conduct, Plaintiff and Class  
13 Members have suffered and will continue to suffer other forms of injury and/or harm.

14 180. Defendant should be compelled to disgorge into a common fund or constructive  
15 trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from  
16 them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and  
17 Class Members overpaid for Defendant's services.

19 **FOURTH COUNT**

20 **Violation of the California Unfair Competition Law**  
21 **[Cal. Bus. & Prof. Code § 17200, *et seq.* – Unlawful Business Practices]**  
**(On Behalf of Plaintiff and the Class)**

22 181. Plaintiff re-alleges and incorporates by reference all prior paragraphs as if fully set  
23 forth herein.

24 182. Ethos violated Cal. Bus. and Prof. Code § 17200, *et seq.*, by engaging in unlawful,  
25 unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading  
26

1 advertising that constitute acts of “unfair competition” as defined in Cal. Bus. Prof. Code § 17200  
2 with respect to the services provided to the Class.

3 183. Ethos engaged in unlawful acts and practices with respect to the services by  
4 establishing the sub-standard security practices and procedures described herein; by soliciting and  
5 collecting Plaintiff’s and Class Members’ PII with knowledge that the information would not be  
6 adequately protected; and by storing Plaintiff’s and Class Members’ PII in an unsecure electronic  
7 environment in violation of California’s data breach statute, Cal. Civ. Code § 1798.81.5, which  
8 requires Ethos to take reasonable methods for safeguarding the PII of Plaintiff and the Class  
9 Members.  
10

11 184. In addition, Ethos engaged in unlawful acts and practices by failing to disclose the  
12 Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code §  
13 1798.82.  
14

15 185. As a direct and proximate result of Ethos’s unlawful practices and acts, Plaintiff  
16 and Class Members were injured and lost money or property, including but not limited to the price  
17 received by Ethos for the products and services, the loss of Plaintiff’s and Class Members’ legally  
18 protected interest in the confidentiality and privacy of their PII, nominal damages, and additional  
19 losses as described herein.  
20

21 186. Ethos knew or should have known that its computer systems and data security  
22 practices were inadequate to safeguard Plaintiff’s and Class Members’ PII and that the risk of a  
23 data breach or theft was highly likely. Ethos’s actions in engaging in the above-named unlawful  
24 practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect  
25 to the rights of Plaintiff and Class Members.  
26  
27

1 187. Plaintiff, on behalf of the Class, seeks relief under Cal. Bus. & Prof. Code § 17200,  
2 *et seq.*, including, but not limited to, restitution to Plaintiff and Class Members of money or  
3 property that Ethos may have acquired by means of its unlawful, and unfair business practices,  
4 restitutionary disgorgement of all profits accruing to Ethos because of its unlawful and unfair  
5 business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. §  
6 1021.5), and injunctive or other equitable relief.

7  
8 **PRAYER FOR RELIEF**

9 **WHEREFORE**, Plaintiff, on behalf of herself and Class Members, requests judgment  
10 against Defendant and that the Court grant the following:

- 11 A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to  
12 represent the Class;
- 13 B. For equitable relief enjoining Defendant from engaging in the wrongful conduct  
14 complained of herein pertaining to the misuse and/or disclosure of the PII of  
15 Plaintiff and Class Members;
- 16 C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive  
17 and other equitable relief as is necessary to protect the interests of Plaintiff and  
18 Class Members, including but not limited to an order:
- 19 i. prohibiting Defendant from engaging in the wrongful and unlawful acts  
20 described herein;
- 21 ii. requiring Defendant to protect, including through encryption, all data collected  
22 through the course of its business in accordance with all applicable  
23 regulations, industry standards, and federal, state or local laws;
- 24 iii. requiring Defendant to delete, destroy, and purge the personal identifying  
25  
26  
27



- 1 information of Plaintiff and Class Members unless Defendant can provide to  
2 the Court reasonable justification for the retention and use of such information  
3 when weighed against the privacy interests of Plaintiff and Class Members;
- 4 iv. requiring Defendant to provide out-of-pocket expenses associated with the  
5 prevention, detection, and recovery from identity theft, tax fraud, and/or  
6 unauthorized use of their PII for Plaintiff's and Class Members' respective  
7 lifetimes;
- 8 v. requiring Defendant to implement and maintain a comprehensive Information  
9 Security Program designed to protect the confidentiality and integrity of the  
10 PII of Plaintiff and Class Members;
- 11 vi. prohibiting Defendant from maintaining the PII of Plaintiff and Class  
12 Members on a cloud-based database;
- 13 vii. requiring Defendant to engage independent third-party security  
14 auditors/penetration testers as well as internal security personnel to conduct  
15 testing, including simulated attacks, penetration tests, and audits on  
16 Defendant's systems on a periodic basis, and ordering Defendant to promptly  
17 correct any problems or issues detected by such third-party security auditors;
- 18 viii. requiring Defendant to engage independent third-party security auditors and  
19 internal personnel to run automated security monitoring;
- 20 ix. requiring Defendant to audit, test, and train its security personnel regarding  
21 any new or modified procedures;
- 22 x. requiring Defendant to segment data by, among other things, creating firewalls  
23 and access controls so that if one area of Defendant's network is compromised,  
24  
25  
26  
27  
28

1 hackers cannot gain access to other portions of Defendant's systems;

2 xi. requiring Defendant to conduct regular database scanning and securing  
3 checks;

4 xii. requiring Defendant to establish an information security training program that  
5 includes at least annual information security training for all employees, with  
6 additional training to be provided as appropriate based upon the employees'  
7 respective responsibilities with handling personal identifying information, as  
8 well as protecting the personal identifying information of Plaintiff and Class  
9 Members;

10  
11 xiii. requiring Defendant to routinely and continually conduct internal training and  
12 education, and on an annual basis to inform internal security personnel how to  
13 identify and contain a breach when it occurs and what to do in response to a  
14 breach;

15  
16 xiv. requiring Defendant to implement a system of tests to assess its respective  
17 employees' knowledge of the education programs discussed in the preceding  
18 subparagraphs, as well as randomly and periodically testing employees'  
19 compliance with Defendant's policies, programs, and systems for protecting  
20 personal identifying information;

21 xv. requiring Defendant to implement, maintain, regularly review, and revise as  
22 necessary a threat management program designed to appropriately monitor  
23 Defendant's information networks for threats, both internal and external, and  
24 assess whether monitoring tools are appropriately configured, tested, and  
25 updated;  
26

1 xvi. requiring Defendant to meaningfully educate all Class Members about the  
2 threats that they face as a result of the loss of their confidential personal  
3 identifying information to third parties, as well as the steps affected  
4 individuals must take to protect themselves;

5 xvii. requiring Defendant to implement logging and monitoring programs sufficient  
6 to track traffic to and from Defendant's servers; and for a period of 10 years,  
7 appointing a qualified and independent third party assessor to conduct a SOC  
8 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance  
9 with the terms of the Court's final judgment, to provide such report to the  
10 Court and to counsel for the class, and to report any deficiencies with  
11 compliance of the Court's final judgment;

12  
13 D. For an award of damages, including actual, nominal, statutory, consequential, and  
14 punitive damages, as allowed by law in an amount to be determined;

15 E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

16 F. For prejudgment interest on all amounts awarded; and

17 G. Such other and further relief as this Court may deem just and proper.  
18

19 **JURY TRIAL DEMANDED**

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

21 Dated: January 11, 2023

Respectfully Submitted,

22 /s/ John Nelson

23 John J. Nelson (SBN 317598)

**MILBERG COLEMAN BRYSON**

**PHILLIPS GROSSMAN PLLC**

401 W Broadway, Suite 1760

San Diego, CA 92101

Tel: (858) 209-6941

[jnelson@milberg.com](mailto:jnelson@milberg.com)

24  
25  
26  
27  
28 CLASS ACTION COMPLAINT

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Ethos Technologies Hit with Class Action Over Months-Long Data Breach](#)

---