Exhibit A

M. ANDERSON BERRY (262879)
aberry@justice4you.com
GREGORY HAROUTUNIAN (330263)
gharoutunian@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829

DYLAN J. GOULD
dgould@msdlegal.com
JONATHAN T. DETERS
jdeters@msdlegal.com
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700
Facsimile: (513) 665-0219

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA - SAN FRANCISCO DIVISION

CHRISTOPHER STEIN, individually, and on behalf of all others similarly situated, Plaintiff, vs. ETHOS TECHNOLOGIES, INC.; GUIDEWIRE SOFTWARE, INC., Defendants.	**Case No.** _____ **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Christopher Stein, individually, and on behalf of all others similarly situated, brings this Class Action Complaint ("Complaint") against Defendants Ethos Technologies, Inc. ("Ethos") and Guidewire Software, Inc. ("Guidewire") (collectively "Defendants"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendants.

Plaintiff makes the following allegations on information and belief, except as to his own actions, which are made on personal knowledge, the investigation of his counsel, and the facts that are a matter of public record.

I. NATURE OF CASE

1. This class action arises out of the recent targeted cyberattack and data breach ("Data Breach") on Ethos's network through its third-party integrated service provider, Guidewire, that resulted in unauthorized access to highly sensitive data.[1] As a result of the Data Breach, Class Members suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the present risk of imminent harm caused by the compromise of their sensitive personal information.

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

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

4. Plaintiff and Class Members' PII—which was entrusted to Defendants, their officials, and agents—was compromised and unlawfully accessed due to the Data Breach.

5. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of his and Class Members' PII that Defendants

[1] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-21.pdf

collected and maintained, and for Defendants' failure to provide timely and adequate notice to Plaintiff and other Class Members that their PII had been subject to the unauthorized access of an unknown, unauthorized party.

6. Defendants maintained the PII in a negligent and/or reckless manner. In particular, the PII was maintained on Defendants' computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendants, and thus Defendants were on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

7. In addition, upon information and belief, Defendants and their employees failed to properly monitor the computer network, IT systems, and integrated service that housed Plaintiff's and Class Members' PII.

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

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

10. In letters dated December 21, 2022, Defendant Ethos notified state Attorneys General and many Class Members about the widespread data breach that had occurred on

Defendant Ethos's computer network and that Class Members' PII was accessed and acquired by malicious actors, using Defendant Guidewire's integrated insurance services.[2]

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

> **What Happened?** Ethos offers life insurance policies through an online application process. On December 8, 2022, we learned that unauthorized actors had launched a sophisticated and successful cyberattack against our website to access certain persons' SSNs. We immediately investigated the incident and made a series of technical changes to our website to prevent further unauthorized access to SSNs. The vast majority of people affected by this incident were not existing Ethos customers.
>
> To access SSNs, the unauthorized actors entered information they had obtained about you from other sources—first and last name, date of birth, and address—into our online insurance application flow. This caused a third-party integrated service to return your SSN to the page source code on our website. Then, the unauthorized actors used specialized tools to extract SSNs from the page source code of our website. Importantly, these SSNs did not appear on the public-facing application page of the site. The incident spanned from approximately August 4, 2022 through December 9, 2022.
>
> **What Information Was Involved?** Social Security number.[3]

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

13. Defendant Ethos's Notice of Security correspondence further admitted that the PII accessed included individuals' names and Social Security numbers.[4]

14. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class

[2] *Id.*
[3] *Id.*
[4] *Id.*

Members' information to target other phishing and hacking intrusions using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

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

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

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

18. Accordingly, Plaintiff brings claims on behalf of himself and the Class for: (i) negligence, (ii) invasion of privacy and (iii) unjust enrichment. Through these claims, Plaintiff seeks, *inter alia*, damages and injunctive relief, including improvements to Defendants' data security systems and integrated services, future annual audits, and adequate credit monitoring services.

II. THE PARTIES

19. Plaintiff Christopher Stein is a natural person, resident, and a citizen of the State of Ohio. Plaintiff Stein has no intention of moving to a different state in the immediate future. Plaintiff Stein is acting on his own behalf and on behalf of others similarly situated. Defendants obtained and continue to maintain Plaintiff Stein's PII and owed him a legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff Stein's PII was compromised

and disclosed as a result of Defendant's inadequate data security, which resulted in the Data Breach.

20. Plaintiff received a notice letter from Ethos dated December 21, 2022, stating that a data security incident occurred at Ethos and Plaintiff's PII was involved in the incident. Upon information and belief, the breach was a result of Guidewire's inadequate integrated services on Ethos's website.

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

22. Defendant Guidewire Software, Inc. provides software systems for companies in the insurance industry. Guidewire is incorporated under the laws of Delaware with its headquarters located at 2850 South Delaware St., Suite 400, San Mateo, California 94403.

III. JURISDICTION AND VENUE

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

24. This Court has personal jurisdiction over Defendants because Defendants and/or their parents or affiliates are headquartered in this District and Defendants conduct substantial business in California and this District through their headquarters, offices, parents, and affiliates.

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

IV. DEFENDANTS' BUSINESSES

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

27. Defendant Guidewire provides software products and services for the global insurance market. Guidewire's software systems are designed to help insurance carriers improve their operational efficiency, speed to market, and customer experience by providing a central source for all customer, transactional, and financial data.

28. On information and belief, Defendants maintain the PII of customers, insurance applicants, and others, including but not limited to:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Medication information;
- Health insurance information;
- Photo identification;
- Employment information, and;
- Other information that Defendants may deem necessary to provide care.

29. Additionally, Defendants may receive PII from other individuals and/or organizations that are part of a customers' "circle of care," such as referring physicians, customers' other doctors, customers' health plan(s), close friends, and/or family Members.

30. Plaintiff and Class Members directly or indirectly entrusted Defendants with sensitive and confidential PII, which includes information that is static, does not change, and can be used to commit myriad financial crimes.

31. Because of the highly sensitive and personal nature of the information Defendants acquire, store, and have access to, Defendants, upon information and belief, promise to, among other things: keep PII private; comply with industry standards related to data security and PII; inform individuals of their legal duties and comply with all federal and state laws protecting PII; only use and release PII for reasons that relate to medical care and treatment; and provide adequate notice to impacted individuals if their PII is disclosed without authorization.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

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

34. Plaintiff and the Class Members relied on Defendants to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use such PII solely for business purposes, and to prevent the unauthorized disclosures of the PII.

V. THE CYBERATTACK

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

36. Defendant Ethos investigated the suspicious activity, and through its investigation determined that its network was subject to a cyber-attack using the integrated service software on

its website. Upon information and belief, that service is provided by Defendant Guidewire. Unauthorized actors used this integrated software to access and acquire PII without authorization.

37. The investigation determined that private information related to certain customers and other individuals on Defendant Ethos's website were accessed and taken by an unauthorized user between August 4, 2022, and December 9, 2022.

38. Upon information and belief, Plaintiff's and Class Members' PII was exfiltrated and stolen in the attack.

39. Upon information and belief, the unauthorized actors were able to plug in consumer information that they had obtained through other sources into Defendant Ethos's insurance application flow on its website. This simple maneuver prompted a return of the named consumers' Social Security numbers in the application. The PII was then accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor.

40. It is likely the Data Breach was targeted at Defendants due to their status as an insurance related service provider that collects, creates, and maintains sensitive PII.

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

42. Defendant Ethos admitted that the stolen information included full names and Social Security Numbers.

43. While Defendant Ethos stated in the notice letter that the unauthorized activity occurred and was discovered on December 8, 2022, Defendants did notify the specific persons or entities whose PII was acquired and exfiltrated until December 21, 2022– over six months after the Data Breach began on August 4, 2022.

///

44. Upon information and belief, and based on the type of cyberattack, it is plausible and likely that Plaintiff's PII was stolen in the Data Breach. Plaintiff further believes his PII was likely subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals.

45. Defendants had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

46. In response to the Data Breach, Defendant Ethos admits they worked with an "independent forensic investigation firm" to determine the nature and scope of the incident and purports to have taken steps to secure the systems. Defendant Ethos admits additional security was required, but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' PII going forward.

47. Because of the Data Breach, data thieves were able to gain access to Defendants' private systems for months (between August 4, 2022, and December 9, 2021) and were able to compromise, access, and acquire the protected PII of Plaintiff and Class Members.

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

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

50. Plaintiff's and Class Members' unencrypted, unredacted PII was compromised due to Defendants' negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' PII. Criminal hackers obtained their PII because of its value in exploiting

and stealing the identities of Plaintiff and Class Members. The risks to Plaintiff and Class Members will remain for their respective lifetimes.

A. The Data Breach was a Foreseeable Risk of which Defendants were on Notice

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

52. In light of recent high profile data breaches at other insurance partner and provider companies, Defendants knew or should have known that their electronic records and PII they maintained would be targeted by cybercriminals and ransomware attack groups.

53. Defendant Ethos knew or should have known that these attacks were common and foreseeable, as it discovered a separate and distinct but substantially similar data breach in January 2022, which also occurred for approximately six months.[5]

54. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[6] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[7]

55. In light of recent high profile cybersecurity incidents within Defendant Ethos's website and at other insurance partners and provider companies, Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

[5] https://www.doj.nh.gov/consumer/security-breaches/documents/ethos-technologies-20220218.pdf

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

[7] *Id.*

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

B. Defendants Fail to Comply with FTC Guidelines

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

58. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.[8] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[9]

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

---

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

[9] *Id*.

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

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

62. Defendants failed to properly implement basic data security practices.

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

64. Defendants were at all times fully aware of their obligation to protect the PII. Defendants were also aware of the significant repercussions that would result from their failure to do so.

C. Defendants Fail to Comply with Industry Standards

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

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

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

68. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation 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, 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 for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

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

VI. DEFENDANTS' BREACH

70. Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and website's application flow. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect PII;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PII it created, received, maintained, and/or transmitted;

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights;

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

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. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access Defendants' 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 also lost the benefit of the bargain they made with Defendant.

A. 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 Defendants are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

74. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[10]

75. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking

[10] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are 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.

technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

76. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[11]

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

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

///

[11] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 19, 2022).

79. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[12]

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

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

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

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

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

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

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

---

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

[13] GAO Report, at p. 29.

86. PII can sell for as much as $363 per record according to the Infosec Institute.[14] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for many years.

87. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[15] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[16] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

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

89. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the

---

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

[15] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (Jan. 19, 2022).

[16] *Id* at 4.

old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

90. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[18]

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

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

B. Plaintiff's and Class Members' Damages

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

94. Defendant Ethos has merely offered Plaintiff and Class Members complimentary fraud and identity monitoring services for up to two years, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach.

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

---

[17] 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.

[18] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card 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.

96. Plaintiff and Class Members' full names and Social Security numbers were compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendants' software maintaining PII. As Defendant Ethos admits, these impacted persons were specifically targeted: the cybercriminals used their names, dates of birth and addresses to steal Plaintiff's and Class Members Social Security numbers.

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

98. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring his accounts for fraudulent activity.

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

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

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

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

103. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could

use that information to more effectively target such schemes to Plaintiff and Class Members. Plaintiff has already experienced fraudulent conduct, as a credit account was opened in his name at Bank of America without his consent and he was forced to place a freeze on his financial and credit accounts.

104. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach. Since learning of the Data Breach, Plaintiff Stein has instituted a credit freeze.

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

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

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

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

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

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

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

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

///

C. Plaintiff Stein's Experience

112. Plaintiff Stein does not know how Defendants obtained his PII and he had never heard of Defendants until he received the breach notice in December 2022.

113. Plaintiff Stein is very careful about sharing his sensitive Private Information. Plaintiff Stein has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

114. Plaintiff Stein first learned of the Data Breach after receiving a data breach notification letter dated December 21, 2022, from Ethos, notifying him that Defendants suffered a data breach for four months prior and that his PII had been improperly accessed and/or obtained by unauthorized third parties while in possession of Defendants.

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

116. As a result of the Data Breach, Plaintiff Stein made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

117. Plaintiff Stein experienced actual identify theft and fraud, which he discovered a financial account was opened at Bank of America using his name. Plaintiff Stein has had to place a credit freeze on his accounts and take significant efforts to remedy his credit file as a result of the Data Breach.

118. Plaintiff Stein has spent multiple hours and will continue to spend valuable time for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff Stein spent significant filing a police report with his local police agency and also filing a report with the FTC's identity theft reporting website.

119. Plaintiff Stein suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendants maintained belonging to Plaintiff Stein; (b) violation of his privacy rights; (c) the theft of his PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

120. As a result of the Data Breach, Plaintiff Stein has also suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Stein is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

121. As a result of the Data Breach, Plaintiff Stein anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Stein will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

VII. CLASS ACTION ALLEGATIONS

122. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated ("the Class").

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

> **All persons identified by Defendants (or their agents or affiliates) as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").**

124. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendants have a controlling interest; and the affiliates, legal representatives,

attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

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

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

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

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their PII;

f. Whether Defendants breached their duty to Class Members to safeguard their PII;

g. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

h. Whether Defendants should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants' breach implied contracts with Plaintiff and Class Members;

l. Whether Defendants were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. Whether Defendants failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

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

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

130. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any

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

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

132. Defendants have acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

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

a. Whether Defendants failed to timely notify the public of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

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

CAUSES OF ACTION

FIRST COUNT
Negligence
(On Behalf of Plaintiff and the Class)

135. Plaintiff re-alleges and incorporates by reference by reference herein all of the allegations contained in paragraphs 1 through 134.

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

137. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

138. By collecting and storing this data in their computer system and network, and sharing it and using it for commercial gain, Defendants owed a duty of care to use reasonable means to secure and safeguard their computer system—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants'

duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

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

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

141. Defendants' duty to use reasonable security measures required Defendants to reasonably protect confidential data from any intentional or unintentional use or disclosure.

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

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

144. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' PII;

f. Failing to detect in a timely manner that Class Members' PII had been compromised; and

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.

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

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

147. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

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

149. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendants hold vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the PII—whether by malware or otherwise.

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

151. Defendants breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and Class Members—which actually and proximately caused the Data Breach and injured Plaintiff and Class Members.

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

153. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their

PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

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

154. Plaintiff re-alleges and incorporates by reference by reference herein all of the allegations contained in paragraphs 1 through 134.

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

156. Defendants owed a duty to Plaintiff and Class Member to keep their PII confidential.

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

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

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

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

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

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

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

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

165. Plaintiff, on behalf of himself and Class Members, seeks injunctive relief to enjoin Defendants from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII.

166. Plaintiff, on behalf of himself and Class Members, seeks compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

///

///

///

THIRD COUNT
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

167. Plaintiff re-alleges and incorporates by reference by reference herein all of the allegations contained in paragraphs 1 through 166.

168. This count is pleaded in the alternative to breach of implied contract.

169. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

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

171. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they purchased goods and services from Defendants and/or their agents and in so doing provided Defendants with their PII. In exchange, Plaintiff and Class Members should have received from Defendants the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

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

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

///

174. Defendants were enriched by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid the data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

175. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

176. Defendants acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

177. If Plaintiff and Class Members knew that Defendants had not secured their PII, they would not have agreed to provide their PII to Defendants.

178. Plaintiff and Class Members have no adequate remedy at law.

179. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued

risk to their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

180. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

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

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendants to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

vi. prohibiting Defendants from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vii. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

xi. requiring Defendants to conduct regular database scanning and securing checks;

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

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

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

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

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

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

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

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

F. For prejudgment interest on all amounts awarded; and

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

///

///

///

JURY TRIAL DEMANDED

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

Dated: December 30, 2022

Respectfully Submitted,

By: */s/ M. Anderson Berry*

M. Anderson Berry
aberry@justice4you.com
Gregory Haroutunian
gharoutunian@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Fax: (916) 924-1829

Dylan J. Gould*
dgould@msdlegal.com
Jonathan T. Deters*
jdeters@msdlegal.com
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700
Fax: (513) 665-0219

* *Pro hac vice forthcoming*

Attorneys for Plaintiff and the Proposed Class

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

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

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

JOHN BLUMENSTOCK, THOMAS ROSSELLO, and JEFFREY BRANCH on behalf of themselves and all others similarly situated, Plaintiffs, v. ETHOS TECHNOLOGIES, INC., Defendant.	Case No. 3:23-cv-00073 **CLASS ACTION COMPLAINT FOR DAMAGES** **JURY TRIAL DEMANDED**

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

INTRODUCTION

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

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

///

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

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

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

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

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

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

9. Using "tools," hackers could then extract consumer information from Ethos' source code.

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

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

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

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

14. Like the first data breach, Ethos did not detect it when it happened, nor would it for four months.

15. And by the time it did, hackers had already pilfered the personal information belonging to thousands of individuals.

16. The information compromised in this second data breach in August 2022 disclosed consumers' "personally identifiable information" ("PII"), including Social Security numbers, and is the breach at issue in this litigation (the "Data Breach").

17. Plaintiffs are Data Breach victims who had no relationship with Ethos but received its breach notice in December 2022, informing them their Social Security numbers were compromised in the Data Breach. They bring this Class Action on behalf of themselves and all others harmed by Ethos' misconduct in causing its August 2022 Data Breach.

PARTIES

18. Plaintiff, John Blumenstock, is a natural person and citizen of Kentucky, residing in Louisville, Kentucky, where he intends to remain. Mr. Blumenstock is a Data Breach victim, receiving Ethos' Breach Notice in December 2022.

19. Plaintiff, Thomas Rossello, is a natural person and citizen of Florida, residing in Pompano Beach, Florida, where he intends to remain. Mr. Rossello is a Data Breach victim, receiving Ethos' Breach Notice in December 2022.

20. Plaintiff, Jeffrey Branch, is a natural person and citizen of Florida, residing in Naples, Florida, where he intends to remain. Mr. Branch is a Data Breach victim, receiving Ethos' Breach Notice in December 2022.

21. Defendant, Ethos, is a corporation with its principal place of business at 75 Hawthorne Street, Suite 2000, San Francisco, California 94105. It is incorporated in Delaware.

JURISDICTION & VENUE

22. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Ethos.

23. Ethos is incorporated in Delaware and maintains its principal place of business in California at 75 Hawthorne Street, Suite 2000, San Francisco, California 94105. Ethos is thus a Delaware and California citizen.

24. This Court has personal jurisdiction over Ethos because it is a citizen in this District and maintains its headquarters and principal place of business in this District.

25. Venue is proper because Ethos maintains its headquarters and principal place of business in this District.

BACKGROUND FACTS

A. Ethos

26. Ethos is a life insurance company that quotes and sells policies online.

27. As an online company dealing in highly sensitive information, Ethos should understand its duties to safeguard personal information.

28. Indeed, Ethos advertises that securing PII is "an integral part" of its mission:

29. The efforts Ethos claims to have implemented include encryption, multi-factor authentication, and "oversight" from third party security companies.

///

///

///

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

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

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

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

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

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

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

B. Ethos Fails to Safeguard Consumer PII

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

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

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

[1] See Ethos' privacy policy at https://www.ethoslife.com/privacy/ (last accessed January 2, 2023).

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

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

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

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

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

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

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

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

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

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

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

C. Plaintiffs' Experiences

i. Plaintiff Blumenstock.

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

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

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

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

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

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

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

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

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

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

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

ii. Plaintiff Rossello

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

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

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

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

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

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

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

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

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

iii. Plaintiff Branch

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

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

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

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

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

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

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

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

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

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

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

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

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

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

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

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

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

accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

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

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

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

E. Defendant failed to adhere to FTC guidelines.

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

///

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

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

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

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

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

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

CLASS ACTION ALLEGATIONS

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

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

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

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

a. **Numerosity**. Plaintiffs are representative of the proposed Class, consisting of thousands of members, far too many to join in a single action;

b. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with Class members' interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

///

iv. Whether Defendant breached contract promises to safeguard Plaintiffs' and the Class's PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiffs and the Class injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

96. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual Plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I

NEGLIGENCE

(ON BEHALF OF PLAINTIFFS AND THE CLASS)

97. Plaintiffs reallege all previous paragraphs as if fully set forth below.

98. Defendant owed to Plaintiffs and other members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

99. Defendant owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and members of the Class's PII by disclosing and providing access to this information to third parties and by failing

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

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

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

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

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

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

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

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

COUNT II

NEGLIGENCE PER SE

(ON BEHALF OF PLAINTIFFS AND THE CLASS)

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

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

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

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

///

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

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

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

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

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

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

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

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

///

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

COUNT III

INVASION OF PRIVACY

(ON BEHALF OF PLAINTIFFS AND THE CLASS)

117. Plaintiffs incorporate by reference all preceding allegations.

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

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

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

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

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

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

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

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

///

///

///

///

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

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

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

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

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

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

COUNT V

DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF

(ON BEHALF OF PLAINTIFFS AND THE CLASSES)

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

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

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

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

a. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiffs and the Classes.

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

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

144. The hardship to Plaintiffs and the Classes if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued.

145. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiffs, the Classes, and the public at large.

PRAYER FOR RELIEF

146. Plaintiffs and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

a. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representative, and appointing their counsel to represent the Class;

b. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

c. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

d. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

e. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

f. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

g. Awarding attorneys' fees and costs, as allowed by law;

h. Awarding prejudgment and post-judgment interest, as provided by law;

i. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

j. Granting such other or further relief as may be appropriate under the circumstances.

///

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

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

Attorney for Plaintiff

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

JOSEPHINE DIBISCEGLIA, on behalf of herself and all others similarly situated, Plaintiff, vs. **ETHOS TECHNOLOGIES, INC.,** Defendant.	Case No.: _____ **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

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

NATURE OF CASE

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

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

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

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

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

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

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

[1] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-21.pdf

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

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

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

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

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

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

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

[2] *Id.*

> incident and made a series of technical changes to our website to prevent further unauthorized access to SSNs. The vast majority of people affected by this incident were not existing Ethos customers.
>
> To access SSNs, the unauthorized actors entered information they had obtained about you from other sources—first and last name, date of birth, and address—into our online insurance application flow. This caused a third-party integrated service to return your SSN to the page source code on our website. Then, the unauthorized actors used specialized tools to extract SSNs from the page source code of our website. Importantly, these SSNs did not appear on the public-facing application page of the site. The incident spanned from approximately August 4, 2022 through December 9, 2022.
>
> **What Information Was Involved?** Social Security number.[3]

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

13. Ethos's Notice letter further admitted that the PII accessed included individuals' names and Social Security numbers.[4]

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

[3] *Id.*
[4] *Id.*

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

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

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

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

THE PARTIES

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

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

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

JURISDICTION AND VENUE

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

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

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

DIVISIONAL ASSIGNMENT

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

DEFENDANT'S BUSINESS

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

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

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Financial information;
- Information relating to individual medical history;
- Information concerning an individual's doctor, nurse, or other medical providers;
- Medication information,
- Health insurance information,
- Photo identification;
- Employment information, and;
- Other information that Defendant may deem necessary to provide care.

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

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

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

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

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

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

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

THE CYBERATTACK

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

54. Moreover, Ethos knew or should have known that these attacks were common and foreseeable, as it discovered a separate and distinct but substantially similar data breach in January 2022, which also occurred for approximately several months.[8]

---

[5] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[6] *Id.*
[7] 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/
[8] https://www.doj.nh.gov/consumer/security-breaches/documents/ethos-technologies-20220218.pdf

55. In light of recent high profile cybersecurity incidents at other insurance partners and provider companies, Ethos knew or should have known that their electronic records would be targeted by cybercriminals.[9]

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

Defendant Fails to Comply with FTC Guidelines

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

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

---

[9] 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/

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

[11] *Id.*

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

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

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

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

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

64. Defendant was at all times fully aware of their obligation to protect the PII. Defendant was also aware of the significant repercussions that would result from their failure to do so.

Defendant Fails to Comply with Industry Standards

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

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

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

68. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation 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, 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 for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

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

DEFENDANT'S BREACH

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

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect PII;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PII it created, received, maintained, and/or transmitted;

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights;

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

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.

74. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[12]

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

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

[12] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are 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.

charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[13]

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

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

79. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[14]

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

---

[13] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 19, 2022).

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

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

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

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

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

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

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

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

---

[15] GAO Report, at p. 29.

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

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

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

89. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[19]

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

[17] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (Jan. 19, 2022).
[18] *Id* at 4.
[19] 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.

card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[20]

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

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

Plaintiff's and Class Members' Damages

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

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

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

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

[20] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

d. Contacting financial institutions and closing or modifying financial accounts; and

e. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

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

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

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

Plaintiff Dibisceglia's Experience

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

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

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

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

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

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

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

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

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

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

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

CLASS ACTION ALLEGATIONS

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

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

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

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

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

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

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

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached implied contracts made with Plaintiff and Class Members;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and,

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

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

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

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

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

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

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

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

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and,

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

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

CAUSES OF ACTION

FIRST COUNT
Negligence
(On Behalf of Plaintiff and the Class)

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

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

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

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

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

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

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

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

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

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

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' PII;

f. Failing to detect in a timely manner that Class Members' PII had been compromised; and,

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

THIRD COUNT
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PRAYER FOR RELIEF

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

A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

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

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying

information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

vi. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised,

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

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

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

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

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

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

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

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

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

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

F. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMANDED

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

Dated: January 11, 2023

Respectfully Submitted,

/s/ *John Nelson*

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

M. ANDERSON BERRY (262879)
aberry@justice4you.com
GREGORY HAROUTUNIAN (330263)
gharoutunian@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829

JOHN J. NELSON (SBN 317598)
jnelson@milberg.com
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN PLLC
401 W Broadway, Suite 1760
San Diego, CA 92101
Telephone: (858) 209-6941

Attorneys for Plaintiffs and Proposed Class

(additional counsel listed on signature page)

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE: ETHOS TECHNOLOGIES, INC. DATA BREACH LITIGATION This Document Relates To: ALL ACTIONS	Case No. 3:22-cv-09203-SK **CONSOLIDATED CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs Christopher Stein, Josephine Dibisceglia, John Blumenstock, Thomas Rossello, Jeffrey Branch, Derrick Carter, Trevor Pearch, James Schneider and Tameka Young, individually, and on behalf of all others similarly situated, bring this Class Action Complaint ("Complaint") against Defendant Ethos Technologies, Inc. ("Ethos") ("Defendant" or "Ethos"),

to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations on information and belief, except as to their own actions, which are made on personal knowledge, the investigation of their counsel, and the facts that are a matter of public record.

I. INTRODUCTION

1. This class action arises out of the recent targeted cyberattack and data breach ("Data Breach") on Ethos' network that resulted in unauthorized access to highly sensitive data.[1] As a result of the Data Breach, Class Members suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the present risk of imminent harm caused by the compromise of their sensitive personal information.

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

3. Upon information and belief, prior to and through December 2022, Defendant obtained the PII of Plaintiffs and Class Members and stored that PII, unencrypted, in an Internet-accessible environment on Defendant Ethos' network, in which unauthorized actors used an extraction tool to retrieve Social Security numbers from Ethos' network.

4. Plaintiffs and Class Members' PII—which were entrusted to Defendant, their officials, and agents—were compromised and unlawfully accessed due to the Data Breach.

5. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of theirs and Class Members' PII that Defendant

[1] *Consumer Notification Letter*, DEPT JUSTICE MONTANA (Dec. 21, 2022) https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-21.pdf.

collected and maintained, and for Defendant's failure to provide timely and adequate notice to Plaintiffs and other Class Members that their PII had been subject to the unauthorized access of an unknown, unauthorized party.

6. Defendant maintained the PII in a negligent and/or reckless manner. In particular, the PII was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

7. In addition, upon information and belief, Defendant and its employees failed to properly monitor the computer network, IT systems, and integrated service that housed Plaintiffs' and Class Members' PII.

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

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

10. In letters dated December 21, 2022, Defendant Ethos notified state Attorneys General and many Class Members about the widespread data breach that had occurred on

Defendant Ethos' computer network and that Class Members' PII was accessed and acquired by malicious actors.[2]

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

> **What Happened?** Ethos offers life insurance policies through an online application process. On December 8, 2022, we learned that unauthorized actors had launched a sophisticated and successful cyberattack against our website to access certain persons' SSNs. We immediately investigated the incident and made a series of technical changes to our website to prevent further unauthorized access to SSNs. The vast majority of people affected by this incident were not existing Ethos customers.
>
> To access SSNs, the unauthorized actors entered information they had obtained about you from other sources—first and last name, date of birth, and address—into our online insurance application flow. This caused a third-party integrated service to return your SSN to the page source code on our website. Then, the unauthorized actors used specialized tools to extract SSNs from the page source code of our website. Importantly, these SSNs did not appear on the public-facing application page of the site. The incident spanned from approximately August 4, 2022 through December 9, 2022.
>
> **What Information Was Involved?** Social Security number.[3]

12. Defendant Ethos acknowledged its investigation into the Data Breach and determined that there was unauthorized access to Plaintiffs' and Class Members' Social Security numbers between August 4, 2022, and December 9, 2022. Defendant Ethos' investigation concluded, and it learned what information was available to the unauthorized actors, on December 8, 2022.

///

///

[2] *Id.*
[3] *Id.*

13. Defendant Ethos' Notice of Security correspondence further admitted that the PII accessed included individuals' names and Social Security numbers.[4]

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

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

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

17. By their Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach.

18. Accordingly, Plaintiffs bring claims on behalf of themselves and the Class for: (i) negligence, (ii) invasion of privacy, (iii) unjust enrichment, (iv) violations of the California Unfair Competition Law, and (v) declaratory judgment and injunctive relief. Through these claims,

[4] *Id.*

Plaintiffs seek, *inter alia*, damages and injunctive relief, including improvements to Defendant's data security systems and integrated services, future annual audits, and adequate credit monitoring services.

II. PARTIES

19. Plaintiff Christopher Stein is a natural person, resident, and citizen of Ohio where he intends to remain. He is a Data Breach victim, having received Ethos' breach notice in December 2022.

20. Plaintiff Josephine Dibisceglia is a natural person, resident, and citizen of Florida where she intends to remain. She is a Data Breach victim, having received Ethos' breach notice in December 2022.

21. Plaintiff John Blumenstock is a natural person, resident, and citizen of Kentucky where he intends to remain. He is a Data Breach victim, having received Ethos' breach notice in December 2022.

22. Plaintiff Thomas Rossello is a natural person, resident, and citizen of Florida where he intends to remain. He is a Data Breach victim, having received Ethos' breach notice in December 2022.

23. Plaintiff Jeffrey Branch is a natural person, resident, and citizen of Florida where he intends to remain. He is a Data Breach victim, having received Ethos' breach notice in December 2022.

24. Plaintiff Derrick Carter is a natural person, resident and citizen of the State of Florida where he intends to remain. Plaintiff Carter is a data breach victim, having received a Notice of Data Security Incident letter from Ethos, dated December 21, 2022, by U.S. Mail.

///

25. Plaintiff Trevor Pearch is a natural person, resident and citizen of the State of California where he intends to remain. Plaintiff Pearch is a data breach victim, having received a Notice of Data Security Incident letter from Ethos, dated December 21, 2022, by U.S. Mail.

26. Plaintiff James Schneider is a natural person, resident and citizen of the State of Massachusetts where he intends to remain. Plaintiff Schneider is a data breach victim, having received a Notice of Data Security Incident letter from Ethos, dated December 21, 2022, by U.S. Mail.

27. Plaintiff Tameka Young is a natural person, resident and citizen of the State of Florida where she intends to remain. Plaintiff Young is a data breach victim, having received a Notice of Data Security Incident letter from Ethos, dated December 21, 2022, by U.S. Mail.

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

III. JURISDICTION AND VENUE

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

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

///

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

IV. BACKGROUND FACTS

A. Defendant's Businesses

32. Defendant Ethos is an insurance carrier, specializing in life insurance.

33. On information and belief, Defendant maintain the PII of customers, insurance applicants, and others, including but not limited to:

a. name, address, phone number and email address;

b. date of birth;

c. demographic information;

d. social Security number;

e. financial information;

f. information relating to individual medical history;

g. information concerning an individual's doctor, nurse, or other medical providers;

h. medication information;

i. health insurance information;

j. photo identification;

k. employment information, and;

l. other information that Defendant may deem necessary to provide care.

///

///

34. Additionally, Defendant may receive PII from other individuals and/or organizations that are part of a customers' "circle of care," such as referring physicians, customers' other doctors, customers' health plan(s), close friends, and/or family Members.

35. Plaintiffs and Class Members directly or indirectly entrusted Defendant with sensitive and confidential PII, which includes information that is static, does not change, and can be used to commit myriad financial crimes.

36. Because of the highly sensitive and personal nature of the information that the Defendant acquires, stores, and has access to. Defendant, upon information and belief, promised to, among other things: keep PII private; comply with industry standards related to data security and PII; inform individuals of their legal duties and comply with all federal and state laws protecting PII; only use and release PII for reasons that relate to medical care and treatment; and provide adequate notice to impacted individuals if their PII is disclosed without authorization.

37. By obtaining, collecting, using, and deriving a benefit from Plaintiffs and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure.

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

39. Plaintiffs and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use such PII solely for business purposes, and to prevent the unauthorized disclosures of the PII.

///

B. Defendant Fails to Safeguard Consumer PII

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

41. Defendant Ethos investigated the suspicious activity, and through its investigation determined that its network was subject to a cyber-attack using the integrated service software on its website. Unauthorized actors used this integrated software to access and acquire PII without authorization.

42. The investigation determined that private information related to certain customers and other individuals on Defendant Ethos' website was accessed and taken by an unauthorized user between August 4, 2022, and December 9, 2022.

43. Upon information and belief, Plaintiffs' and Class Members' PII was exfiltrated and stolen in the attack.

44. Upon information and belief, the unauthorized actors were able to plug in consumer information that they had obtained through other sources into Defendant Ethos' insurance application flow on its website. This simple maneuver prompted a return of the named consumers' Social Security numbers in the application. The PII was then accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor.

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

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

///

47. Defendant Ethos admitted that the stolen information included full names and Social Security Numbers.

48. While Defendant Ethos stated in the notice letter that the unauthorized activity occurred and was discovered on December 8, 2022, Defendant did notify the specific persons or entities whose PII was acquired and exfiltrated until December 21, 2022—over six months after the Data Breach began on August 4, 2022.

49. Upon information and belief, and based on the type of cyberattack, it is plausible and likely that Plaintiffs' PII was stolen in the Data Breach. Plaintiffs further believe their PII was likely subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals.

50. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

51. In response to the Data Breach, Defendant Ethos admits it worked with an "independent forensic investigation firm" to determine the nature and scope of the incident and purports to have taken steps to secure the systems. Defendant Ethos admits additional security was required, but there is no indication whether these steps are adequate to protect Plaintiffs' and Class Members' PII going forward.

52. Because of the Data Breach, data thieves were able to gain access to Defendant's private systems for months—between August 4, 2022, and December 9, 2021—and were able to compromise, access, and acquire the protected PII of Plaintiffs and Class Members.

53. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their PII confidential and to protect them from unauthorized access and disclosure.

54. Plaintiffs and Class Members reasonably relied (directly or indirectly) on these sophisticated parties to keep their sensitive PII confidential; to maintain proper system security; to use this information for business purposes only; and to make only authorized disclosures of their PII.

55. Plaintiffs' and Class Members' unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' PII. Criminal hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The risks to Plaintiffs and Class Members will remain for their respective lifetimes.

C. The Data Breach was a Foreseeable Risk and Defendant were on Notice

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

57. In light of recent high profile data breaches at other insurance partner and provider companies, Defendant knew or should have known that their electronic records and PII they maintained would be targeted by cybercriminals and ransomware attack groups.

58. Defendant Ethos knew or should have known that these attacks were common and foreseeable, as it discovered a separate and distinct but substantially similar data breach in January 2022, which also occurred for approximately six months.[5]

///

[5] *Breach Notice*, DEPT JUSTICE NEW HAMPSHIRE, (Feb. 11, 2022) https://www.doj.nh.gov/consumer/security-breaches/documents/ethos-technologies-20220218.pdf.

59. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[6] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[7]

60. In light of recent high profile cybersecurity incidents within Defendant Ethos' website and at other insurance partners and provider companies, Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

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

D. Defendant Fails to Comply with FTC Guidelines

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

63. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security

[6] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[7] *Id.*

problems.[8] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[9]

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

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

66. These FTC enforcement actions include actions against insurance providers and partners like Defendant.

67. Defendant failed to properly implement basic data security practices.

///

///

[8] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Feb. 23, 2023).
[9] *Id*.

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

69. Defendant was at all times fully aware of their obligation to protect the PII. Defendant was also aware of the significant repercussions that would result from their failure to do so.

E. Defendant Fails to Comply with Industry Standards

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

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

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

73. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation 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,

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 for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

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

F. Defendant's Breach

75. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and website's application flow. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. failing to adequately protect PII;

c. failing to properly monitor their own data security systems for existing intrusions;

d. failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures;

e. failing to ensure the confidentiality and integrity of electronic PII it created, received, maintained, and/or transmitted;

f. failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights;

g. failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

h. failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

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 Plaintiffs' and Class Members' PII.

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

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

G. Data Breaches Cause Disruption and Increased Risk of Fraud and Identity Theft

78. 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.

79. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[10]

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

---

[10] *See* U.S. GOV. ACCOUNTING OFFICE, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007) https://www.gao.gov/new.items/d07737.pdf.

81. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[11]

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

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

84. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[12]

///

---

[11] *See IdentityTheft.gov*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Steps (last visited Feb. 23, 2023).

[12] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

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

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

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

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

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

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

90. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

---

[13] GAO Report, at p. 21.

91. PII can sell for as much as $363 per record according to the Infosec Institute.[14] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for many years.

92. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[15] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[16] Each of these fraudulent activities is difficult to detect. An individual may not know that their Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

93. Moreover, it is not an easy task to change or cancel a stolen Social Security Number.

94. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the

---

[14] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[15] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION (2018) at 1, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Feb. 23, 2023).

[16] *Id* at 4.

old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

95. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[18]

96. Because of the value of its collected and stored data, the insurance industry has experienced disproportionally higher numbers of data theft events than other industries.

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

H. Plaintiffs' and Class Members' Damages

98. To date, Defendant has done nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

99. Defendant Ethos has merely offered Plaintiffs and Class Members complimentary fraud and identity monitoring services for up to two years, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach.

///

---

[17] 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.

[18] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card 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.

100. Plaintiffs and Class Members have been damaged by the compromise of their PII in the Data Breach.

101. Plaintiffs and Class Members' full names and Social Security numbers were compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's software maintaining PII. As Defendant Ethos admits, these impacted persons were specifically targeted: the cybercriminals used their names, dates of birth and addresses to steal Plaintiffs' and Class Members Social Security numbers.

102. Since being notified of the Data Breach, Plaintiffs have spent time dealing with the impact of the Data Breach, valuable time Plaintiffs otherwise would have spent on other activities, including but not limited to work and/or recreation.

103. Due to the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring their accounts for fraudulent activity.

104. Plaintiffs' PII was compromised as a direct and proximate result of the Data Breach.

105. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

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

///

///

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

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

109. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach. Since learning of the Data Breach, Plaintiff Stein has instituted a credit freeze.

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

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

112. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and sensitive information for misuse.

113. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket

expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. purchasing credit monitoring and identity theft prevention;

c. placing "freezes" and "alerts" with reporting agencies;

d. spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. contacting financial institutions and closing or modifying financial accounts; and

f. closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

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

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

///

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

Plaintiff Stein's Experience

117. Plaintiff Stein does not know how Defendant obtained his PII and he had never heard of Defendant until he received the breach notice in December 2022.

118. Plaintiff Stein is very careful about sharing his sensitive Private Information. Plaintiff Stein has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

119. Plaintiff Stein first learned of the Data Breach after receiving a data breach notification letter dated December 21, 2022, from Ethos, notifying him that Defendant suffered a data breach for four months prior and that his PII had been improperly accessed and/or obtained by unauthorized third parties while in possession of Defendant.

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

121. As a result of the Data Breach, Plaintiff Stein made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

122. Plaintiff Stein experienced actual identify theft and fraud, which includes discovering a financial account was opened at Bank of America using his name. In November 2022, an unauthorized third party used Plaintiff's Social Security number and name to fraudulently apply for a Bank Of America credit card. The fraudulent application was successful,

and the credit card was issued to the fraudster with a limit of $28,500.00. It was mailed to a fraudulent address in Florida, far from Plaintiff's home in Ohio. Plaintiff Stein placed credit freezes on his files with all three credit agencies.

123. Plaintiff Stein has spent multiple hours and will continue to spend valuable time for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation. As such, Plaintiff has spent significant time trying to mitigate the breach by, *inter alia*:

a. filing a police report with his local police agency;

b. filing a report with the FTC's identity theft reporting website;

c. placing a credit freeze on his accounts; and

d. taking significant efforts to remedy his credit file.

124. Plaintiff Stein suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff Stein; (b) violation of his privacy rights; (c) the theft of his PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

125. As a result of the Data Breach, Plaintiff Stein has also suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Stein is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

///

126. As a result of the Data Breach, Plaintiff Stein anticipates spending considerable time and money on an ongoing basis

127. to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Stein will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

Plaintiff Dibisceglia's Experience

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

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

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

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

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

133. Plaintiff Dibisceglia experienced actual identify theft and fraud in or about December 2022, including:

a. over seven thousand dollars of fraudulent charges being placed on her credit card; and;

b. identity thieves attempting to open additional credit cards falsely under her name.

134. Plaintiff Dibisceglia has taken significant efforts to remedy her credit file as a result of the Data Breach.

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

136. Plaintiff Dibisceglia suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant maintained belonging to Plaintiff Dibisceglia; (b) violation of her privacy rights; (c) the theft of her PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

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

///

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

Plaintiff Blumenstock's Experience

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

140. Plaintiff Blumenstock experienced actual identify theft and fraud, including having $6,800 stolen from his Wells Fargo account on or about December 8, 2022by criminals using his exposed PII.

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

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

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

///

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

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

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

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

Plaintiff Rossello's Experience

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

149. Indeed, following the Data Breach, Mr. Rossello suffered identity theft and fraud repeatedly, including:

a. Bank of America called him on or about November 3, 2022 to verify a payment card someone tried to open in his name without his authorization;

b. receiving a similar call from JP Morgan Chase on or about November 3, 2022 seeking to verify a credit card he never opened or authorized;

c. discovering—upon reviewing his credit report on or about November 3, 2022—that there was a hard inquiry from Pentagon Credit Union that he did not authorize; and;

d. having someone try to open a credit card in his name on or about November 3, 2022, specifically, criminals tried to open a credit card in his name *13 times* with Check Systems.

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

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

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

153. Plaintiff Rossello has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff Rossello fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff Rossello has and

is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

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

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

Plaintiff Branch's Experience

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

157. Plaintiff Branch experienced actual identify theft and fraud, including:

a. unauthorized individuals opened two bank accounts in Plaintiff Branch's name at the First National Bank of Omaha on or about December 20, 2022; and

b. such unauthorized individuals accessed other accounts belonging to him between December 20 and 28, 2022 to transfer approximately $60,000 from his accounts to the fraudulent First National Bank of Omaha accounts;

i. $25,000 was transferred on December 20, 2022;

ii. $5,000 was transferred on December 20, 2022; and

iii. $30,000 was transferred on December 28, 2022.

158. As a result, he has spent the better part of two days attempting to remediate the harm this identity theft and fraud has caused him.

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

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

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

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

///

///

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

Plaintiff Carter's Experience

164. Upon information and belief, Defendant obtained Plaintiff Carter's PII when Plaintiff applied for life insurance.

165. Plaintiff Carter's PII was compromised in Ethos' second data breach, compromising his Social Security number and exposing him to identity theft and fraud.

166. Plaintiff Carter trusted that his PII would be safeguarded according to internal policies and state and federal law.

167. Had Plaintiff Carter known of Defendant's security failures, Plaintiff Carter would not have entrusted his PII to Defendant. As a result of the Data Breach, Plaintiff Carter experienced actual identify theft and fraud, including an unknown address showing up on his credit report in late August of 2022.

168. As a result, he has spent at least 4 hours attempting to remediate the harm this identity theft and fraud has caused him, including verifying the legitimacy of the Notice of Data Breach Letter, freezing his credit, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

169. Shortly after and as a result of the Data Breach, Plaintiff Carter began experiencing an increase in spam and suspicious phone calls, texts, and emails.

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

171. Plaintiff Carter has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff Carter fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. This worry goes far

beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

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

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

Plaintiff Young's Experience

174. Upon information and belief, Defendant obtained Plaintiff Young's PII when Plaintiff applied for life insurance.

175. Plaintiff Young's PII was compromised in Ethos' second data breach, compromising her Social Security number and exposing her to identity theft and fraud.

176. Plaintiff Young trusted that her PII would be safeguarded according to internal policies and state and federal law.

177. Had Plaintiff Young known of Defendant's security failures, Plaintiff Young would not have entrusted her PII to Defendant.

178. As a result of the Data Breach, Plaintiff Young experienced actual identity theft and fraud, including:

a. multiple fraudulent charges on two of her bank accounts.

i. As a result of these Fraudulent Charges, in November of 2022, one of her banks restricted her use of the credit card use.

ii. The other institution, in January of 2023, locked her account after notifying her that someone was fraudulently attempting to transfer money out of her account.

b. numerous emails from reputable lending institutions requesting that Plaintiff Young finish loan applications, which she never commenced.

179. As a result of the Breach and resulting identity thefts, Plaintiff Young has suffered credit issues. Specifically, in December of 2022, her application for a new credit card was rejected due to too many recent credit inquiries. These credit inquiries are suspicious and likely fraudulent as Plaintiff Young has applied for new lines of credit only two times in the past 12 months.

180. As a result of these Fraudulent Charges, Plaintiff Young has had to borrow money from relatives and spend numerous hours speaking with her bank's fraud department and is still in the process of fixing these problems.

181. Shortly after and as a result of the Data Breach, Plaintiff Young experienced an increase in spam and suspicious phone calls, texts, and emails.

182. As a result of the Data Breach, Plaintiff Young has spent more than 35 hours dealing with the identity theft, fraud, and other consequences of the Data Breach, including which include time spent verifying the legitimacy of the Notice of Data Breach Letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

183. Plaintiff Young does not recall ever learning that her information was compromised in a data breach incident, other than the breach at issue in this case.

184. Plaintiff Young has and will spend considerable time and effort monitoring her accounts to protect himself from identity theft. Plaintiff Young fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. This worry goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

185. Plaintiff Young is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third

parties. This injury was worsened by Defendant's delay in informing Plaintiffs and Class Members about the Data Breach.

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

Plaintiff Schneider's Experience

187. Upon information and belief, prior to the Data Breach, Defendant obtained Plaintiff Schneider's PII when Plaintiff applied for life insurance.

188. Plaintiff Schneider trusted that his Private Information would be safeguarded according to internal policies and state and federal law.

189. Had Plaintiff Schneider known of Defendant's security failures, he would not have entrusted his PII to Defendant.

190. Upon information and belief, Defendant obtained Plaintiff Young's PII when Plaintiff applied for life insurance.

191. As a result of the Data Breach, Plaintiff Schneider experienced actual identify theft and fraud, including at the end of November 2022, two reputable financial institutions sent him letters informing him that an unauthorized party attempted to open an account in his name to obtain a line of credit.

192. Shortly after and as a result of the Data Breach, Plaintiff Schneider experienced an increase in spam and suspicious phone calls, texts, and emails.

193. As a result of the Data Breach, Plaintiff Schneider has spent time dealing with the identity theft, fraud, and other consequences of the Data Breach, including which include time spent verifying the legitimacy of the Notice of Data Breach Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

///

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

195. Plaintiff Schneider has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff Schneider fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. This worry goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

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

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

Plaintiff Pearch's Experience

198. Despite never forming or seeking a relationship with Ethos, Plaintiff Pearch's PII was compromised in Ethos' second data breach, compromising his Social Security number and exposing him to identity theft and fraud.

199. Plaintiff Branch experienced actual identify theft and fraud, including:

a. fraud when his debit card was accessed on December 17, 2022 and over $8,500 was taken from his checking account;

b. fraud when his debit card was accessed on December 17, 2022 and over $8,500 was taken from his checking account;

///

c. identity theft when he received a letter in December of 2022 from a reputable financial institution informing him that an unauthorized party attempted to open an account in his name; and,

d. actual injury in the form of identity theft when in August of 2022, Plaintiff Branch discovered that unauthorized parties had opened numerous Turbo Tax accounts in his name.

200. As a result of the fraud on his debit card, Plaintiff Pearch's checking account was also overdrawn, and he was assessed resulting fees.

201. As a result of the fraud on his debit card, Plaintiff Pearch lost access to his debit card.

202. As a result of the fraud on his debit card, Plaintiff Pearch was unable to pay numerous bills in the following months, was forced to borrow money and seek funds—from friends and family—which was a source of embarrassment.

203. Shortly after and as a result of the Data Breach, Plaintiff Pearch experienced an increase in spam and suspicious phone calls, texts, and emails.

204. As a result of the Data Breach, Plaintiff Pearch purchased credit monitoring services from Experian, the cost of which was reasonable and necessary.

205. As a result of the fraud and identity theft stemming from the Data Breach, Plaintiff Perch has spent more than two days attempting to remediate the harm this identity theft and fraud has caused him.

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

///

207. Plaintiff Pearch has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff Pearch fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

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

209. Plaintiff Pearch has and will spend more than 50 hours and missed approximately five days of work as a result of responding to the consequences of the Data Breach, including monitoring his accounts to protect himself from identity theft. Plaintiff Pearch fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. This worry goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

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

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

V. CLASS ACTION ALLEGATIONS

212. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

213. Plaintiffs propose the following Class and Subclass definitions, subject to amendment as appropriate:

> **All persons identified by Defendant (or its agents or affiliates) as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").**
>
> **All persons identified by Defendant (or its agents or affiliates) as being among those individuals residing in California impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "California Subclass").**

214. Collectively the Class and California Subclass are referred to as the Classes.

215. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

216. Plaintiffs reserve the right to amend or modify the Class or Subclass definitions as this case progresses.

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

///

///

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

a. if Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. if Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. if Defendant owed a duty to Class Members to safeguard their PII;

f. if Defendant breached their duty to Class Members to safeguard their PII;

g. if Defendant knew or should have known that their data security systems and monitoring processes were deficient;

h. if Defendant should have discovered the Data Breach sooner;

i. if Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. if Defendant's conduct was negligent;

k. if Defendant's breach implied contracts with Plaintiffs and Class Members;

l. if Defendant were unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

m. if Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. if Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

219. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

220. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

221. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

222. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual

Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

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

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

a. if Defendant failed to timely notify the public of the Data Breach;

b. if Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. if Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. if Defendant's failure to institute adequate protective security measures amounted to negligence;

e. if Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

f. if adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

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

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

226. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 224.

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

228. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

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

///

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

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

232. Defendant's duty to use reasonable security measures required Defendant to reasonably protect confidential data from any intentional or unintentional use or disclosure.

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

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

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

a. failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. failing to adequately monitor the security of their networks and systems;

d. failing to have in place mitigation policies and procedures;

e. allowing unauthorized access to Class Members' PII;

f. failing to detect in a timely manner that Class Members' PII had been compromised; and

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.

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

237. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

238. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

///

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

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

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

242. Defendant breached its duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiffs and Class Members—which actually and proximately caused the Data Breach and injured Plaintiffs and Class Members.

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

244. Defendant's breach of its common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiffs and Class Members

actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Invasion of Privacy
(On behalf of the Plaintiffs and the Class)

245. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 224.

246. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

247. Defendant owed a duty to Plaintiffs and Class Member to keep their PII confidential.

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

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

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

251. Defendant knowingly did not notify Plaintiffs and Class Members in a timely fashion about the Data Breach.

252. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

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

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

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

256. Plaintiffs, on behalf of themselves and Class Members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' PII.

257. Plaintiffs, on behalf of themselves and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

258. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 224.

259. This count is pleaded in the alternative to breach of implied contract.

260. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

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

262. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and/or its agents and in so doing provided Defendant with their PII. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

263. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

264. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by paying Defendant as part of Defendant rendering insurance related services, a portion of which was to have been used for data security measures to secure Plaintiffs' and Class Members' PII, and by providing Defendant with their valuable PII.

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

266. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

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

268. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

269. Plaintiffs and Class Members have no adequate remedy at law.

270. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent

researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

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

FOURTH CAUSE OF ACTION
Violation of the California Unfair Competition Law
[Cal. Bus. & Prof. Code § 17200, et seq. – Unlawful Business Practices]
(On Behalf of Plaintiffs and the Class)

273. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 224.

274. Ethos violated Cal. Bus. and Prof. Code § 17200, et seq., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Class.

275. Ethos engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Class Members' PII with knowledge that the information would not

be adequately protected; and by storing Plaintiffs' and Class Members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Ethos to take reasonable methods for safeguarding the PII of Plaintiffs and the Class Members.

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

277. As a direct and proximate result of Ethos' unlawful practices and acts, Plaintiffs and Class Members were injured and lost money or property, including but not limited to the price received by Ethos for the products and services, the loss of Plaintiffs' and Class Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described herein.

278. Ethos knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' PII and that the risk of a data breach or theft was highly likely. Ethos' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

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

FIFTH CAUSE OF ACTION
Declaratory Judgment and Injunctive Relief
(On Behalf of Plaintiffs and the Class)

280. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 224.

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

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

283. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

///

///

b. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiffs and the Classes.

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

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

286. The hardship to Plaintiffs and the Classes if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued.

287. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiffs, the Classes, and the public at large.

///

SIXTH CAUSE OF ACTION
Violation of California's Consumer Privacy Act, Cal. Civ. Code. § 1798.100, *et seq*.
(On Behalf of Plaintiff Trevor Pearch and the California Subclass)

288. Plaintiff Trevor Pearch and the California Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 224.

289. Defendant violated sections 1798.81.5(b) and 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff's and the California Subclass's nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and the California Subclass.

290. As a direct and proximate result of Defendant's acts and violations of their duty under the CCPA, Plaintiff's and the California Subclass's non-redacted and non-encrypted PII was subjected to unauthorized access and exfiltration, theft, or disclosure through Defendant's computer systems.

291. As a direct and proximate result of Defendant's acts, Plaintiff and the California Subclass were injured and lost money or property, including but not limited to the loss of the California Subclass's legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

292. Defendant knew or should have known that their computer systems and data security practices were inadequate to safeguard the California Subclass's PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California Subclass.

293. Defendant is organized or operated for the profit or financial benefit of its shareholders. Defendant collected Plaintiff's and California Subclass Members' PII as defined in Cal. Civ. Code § 1798.140.

294. The PII taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and the California Subclass Members' unencrypted first and last names and Social Security numbers among other information.

295. Plaintiff and the California Subclass Members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

296. At this time, Plaintiff and the California Subclass seek injunctive or other equitable relief to ensure that Defendants hereinafter adequately safeguard PII by implementing reasonable security procedures and practices. This relief is important because Defendant still holds PII related to Plaintiff and the California Subclass. Plaintiff and the California Subclass have an interest in ensuring that their PII is reasonably protected.

297. Pursuant to § 1798.150(b) of the CCPA, on March 1, 2023, Plaintiff Trevor Pearch separately provided written notice to Defendant identifying the specific provisions of this title he alleges it has violated. If within 30 days of Plaintiff's written notice to Defendant it fails to "actually cure" its violations of Cal. Civ. Code § 1798.150(a) and provide "an express written statement that the violations have been cured and that no further violations shall occur," Plaintiff will amend this complaint to also seek the greater of statutory damages in an amount no less than one hundred dollars ($100) and up to seven hundred and fifty ($750) per consumer per incident

or actual damages, whichever is greater, on behalf of the California Subclass. See Cal. Civ. Code § 1798.150(b).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members;

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

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the

retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

vi. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network

is compromised, hackers cannot gain access to other portions of Defendant's systems;

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

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

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

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

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats,

both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

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

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

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

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

F. For prejudgment interest on all amounts awarded; and

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

///

///

JURY TRIAL DEMANDED

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: March 2, 2023,

Respectfully Submitted,

By: */s/ M. Anderson Berry*

M. Anderson Berry
aberry@justice4you.com
Gregory Haroutunian
gharoutunian@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL CORP.
865 Howe Avenue
Sacramento, CA 95825
T: (916) 239-4778
F: (916) 924-1829

Dylan J. Gould*
dgould@msdlegal.com
Jonathan T. Deters*
jdeters@msdlegal.com
MARKOVITS, STOCK &
DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
T: (513) 651-3700
F: (513) 665-0219

Samuel J. Strauss*
sam@turkestrauss.com
Raina Borrelli*
raina@turkestrauss.com
Brittany Resch*
brittanyr@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
T: (608) 237-1775
F: (608) 509-4423

Jean S. Martin*
jeanmartin@forthepeople.com
MORGAN & MORGAN COMPLEX
LITIGATION GROUP

201 N. Franklin Street, 67th Floor
Tampa, FL 33602
TEL: (813)559-4908
FAX: (813) 222-4795

* *Pro hac vice forthcoming*

Attorneys for Plaintiffs and Proposed Class