UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA

ESTHER HICKS, on behalf of herself and all others similarly situated, Plaintiff, v. **CNO FINANCIAL GROUP, INC.** **-and-** **WASHINGTON NATIONAL INSURANCE COMPANY,** Defendants.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Esther Hicks ("Plaintiff"), individually and on behalf of all similarly situated persons, alleges the following against CNO Financial Group, Inc. ("CNO") and Washington National Insurance Company ("Washington National") (collectively, "Defendants") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard Plaintiff's and other similarly situated customers' name, Social Security number, date of birth, and policy number(s) (the "Private Information") from hackers.

2. On or about January 26, 2024, Washington National filed official notice of a hacking incident with the Office of the Maine Attorney General – one of multiple CNO subsidiaries to do so.[1]

3. On or about January 26, 2024, Washington National also sent out data breach letters to individuals whose information was compromised as a result of the hacking incident.

4. Based on the Notice filed by the company, on November 29, 2023, Defendants "discovered that a sophisticated threat actor targeted the cellular account belonging to a company senior officer" via "SIM swapping." As a result of the cyberattack, Washington National and other subsidiary entities of CNO detected unusual activity on their computer systems which, upon information and belief, originated from the CNO senior officer's SIM swap, and launched an investigation revealing that an unauthorized party had access to certain CNO files that contained over 66,000 individuals' Private Information (the "Data Breach").

5. Plaintiff and "Class Members" (defined below) were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm as a result of Defendants' Data Breach. The risk will remain for their respective lifetimes.

6. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, Social Security numbers and policy number(s) that Defendants collected and maintained.

7. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical

[1] *See* Washington National Notice, https://apps.web.maine.gov/online/aeviewer/ME/40/fb22094e-0892-4719-8434-424f1d565d23.shtml; *see also* Bankers Life and Casualty Company Notice, https://apps.web.maine.gov/online/aeviewer/ME/40/1c0e29fa-a97f-4b3e-bd73-4f20e205b77f.shtml (last visited Feb. 9, 2024)

services, 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.

8. There has been no assurance offered by Defendants that all personal data or copies of data have been recovered or destroyed, or that Defendants have adequately enhanced their data security practices sufficient to avoid a similar breach of their network in the future.

9. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

10. Plaintiff brings this class action lawsuit to address Defendants' inadequate safeguarding of Class Members' Private Information that it collected and maintained.

11. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take necessary steps to secure the Private Information left them vulnerable to an attack.

12. Upon information and belief, Defendants failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information. Had Defendants properly monitored their networks, they would have discovered the Breach sooner.

13. Plaintiff's and Class Members' identities are now at risk because of Defendants' negligent conduct as the Private Information that they collected and maintained is now in the hands of data thieves and other unauthorized third parties.

14. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

15. Accordingly, Plaintiff, on behalf of herself and the Class, asserts claims for Negligence, Negligence *Per Se*, Breach of Contract, Breach of Implied Contract, Unjust Enrichment, and Declaratory Judgment. On behalf of herself and the California Subclass (defined below), Plaintiff asserts claims pursuant to violations of the California Consumer Privacy Act, California Unfair Competition Act, and California Legal Remedies Act.

II. PARTIES

16. Plaintiff Hicks is, and at all times mentioned herein was, an individual citizen of the State of California.

17. Defendant Washington National Insurance Company is a supplemental health and life insurance company with its principal place of business at 11825 N. Pennsylvania Street, Carmel, Indiana, 46032 in Hamilton County. Washington National Insurance Company is a subsidiary of CNO Financial Group, Inc.

18. Defendant CNO Financial Group, Inc. is an insurance and financial services company incorporated in Delaware with its principal place of business at 11825 N. Pennsylvania Street, Carmel, Indiana, 46032 in Hamilton County. CNO Financial Group, Inc. is the parent company of Washington National Insurance Company and other subsidiary entities also impacted by the Data Breach.

III. JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has jurisdiction over Defendants because Defendants operate in and are incorporated in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Defendants have harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Defendants' Business and Collection of Plaintiff's and Class Members' Private Information

22. Washington National is a supplemental health and life insurance company that provides insurance policies and products to protect its customers at every stage of life. Founded in 1911, Washington National provides services to individuals, families, business owners, agents, and brokers serving thousands of customers in Indiana and various other states. Washington National is a wholly owned subsidiary of CNO Financial Group Inc.[2]

23. As a condition of receiving supplemental health and life insurance services, Defendants require all Washington National customers to entrust them with highly sensitive

[2] *See* https://ir.cnoinc.com/news/news-details/2021/Washington-National-Offers-New-Life-Insurance-with-Monthly-Income-Protection/default.aspx (last visited Feb. 9, 2024).

personal information. In the ordinary course of receiving service from Defendants, Plaintiff and Class Members were required to provide their Private Information to them.

24. Defendants use this information, *inter alia*, for business, commercial, research, and advertising purposes.

25. In its Insurance Customer Privacy Policy, Washington National informs its customers that it "take[s] your privacy seriously."[3] Washington National also states: "We limit access to our buildings and our information systems to authorized persons. We have policies, procedures and training designed to keep PII safe and secure. We use privacy and security safeguards that meet state and federal regulations."[4]

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

27. Plaintiff and Class Members relied on Defendants to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendants ultimately failed to do.

B. The Data Breach and Defendants' Inadequate Notice to Plaintiff and Class Members

28. According to Defendants' Notice, they learned of unauthorized access to their computer systems on November 29, 2023, with such unauthorized access having taken place on an undisclosed date.

[3] *See* https://washingtonnational.com/insurance-customer-privacy-notice/ (last visited Feb. 9, 2024).
[4] *Id.*

29. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including customers' "name, Social Security number, date of birth, and policy number(s)."

30. On or about January 26, 2024, roughly two months after Defendants learned that the Class's Private Information was first accessed by cybercriminals, Defendants finally began to notify customers that their investigation determined that the Private Information was affected.

31. Washington National delivered Data Breach Notification Letters to Plaintiff and Class Members, alerting them that their highly sensitive Private Information had been exposed in an "event."

32. The notice letter then attached some pages entitled "Recommended Steps to Help Protect Your Information," which listed generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Other than providing one year of crediting monitoring that Plaintiff and Class Members would have to affirmatively sign up for and a call center number that victims could contact "with any questions," Defendants offered no other substantive steps to help victims like Plaintiff and Class Members to protect themselves. On information and belief, CNO sent a similar generic letter to all individuals affected by the Data Breach through other subsidiary entities.

33. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

34. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their

obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

35. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

36. Defendants knew or should have known that their electronic records would be targeted by cybercriminals.

C. Defendants Failed to Comply with FTC Guidelines

37. 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. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

38. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity 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 their network's vulnerabilities, and implement policies to correct any security problems. 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 into 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.

39. The FTC further recommends that companies not maintain personally identifiable information ("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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

40. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

41. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

42. Defendants were, at all times, fully aware of their obligation to protect the Private Information of their customers yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so.

D. Defendants Failed to Comply with Industry Standards

43. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

44. Some industry best practices that should be implemented by businesses like Defendants include but are not limited to educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-

factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

45. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

46. 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.

47. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

E. Defendants Breached their Duty to Safeguard Plaintiff's and Class Members' Private Information

48. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiff and Class Members to provide reasonable security, including complying with

industry standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

49. 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 data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect customers' Private Information;

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

d. Failing to sufficiently train their employees regarding the proper handling of their customers Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' Private Information.

50. Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access their computer network and systems which contained unsecured and unencrypted Private Information.

51. Had Defendants remedied the deficiencies in their information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in

the field, they could have prevented intrusion into their information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

52. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with Defendants.

F. Defendants Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft

53. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[5] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

54. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal 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 or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

[5] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Feb. 9, 2024).

55. 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 to 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.

56. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

57. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

58. One such example of this is the development of "Fullz" packages.

59. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach 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.

60. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen 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 Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen Private Information are being misused, and that such misuse is fairly traceable to the Data Breach.

61. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[6] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

62. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security

[6] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Feb. 9, 2024).

number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

63. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

64. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[7] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendants' industry.

65. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[8] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[9]

---

[7] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military (last visited on Feb. 9, 2024).

[8] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on Feb. 9, 2024).

[9] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on Feb. 9, 2024).

66. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[10]

67. The Dark Web Price Index of 2022, published by PrivacyAffairs[11] shows how valuable just email addresses alone can be, even when not associated with a financial account:

Email Database Dumps	**Avg. Price USD (2022)**
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

68. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

69. Likewise, the value of PII is increasingly evident in our digital economy. Many companies, including Defendants collect PII for purposes of data analytics and marketing. These

[10] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on Feb. 9, 2024).

[11] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited on Feb. 9, 2024).

companies, collect it to better target customers, and shares it with third parties for similar purposes.[12]

70. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[13]

71. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

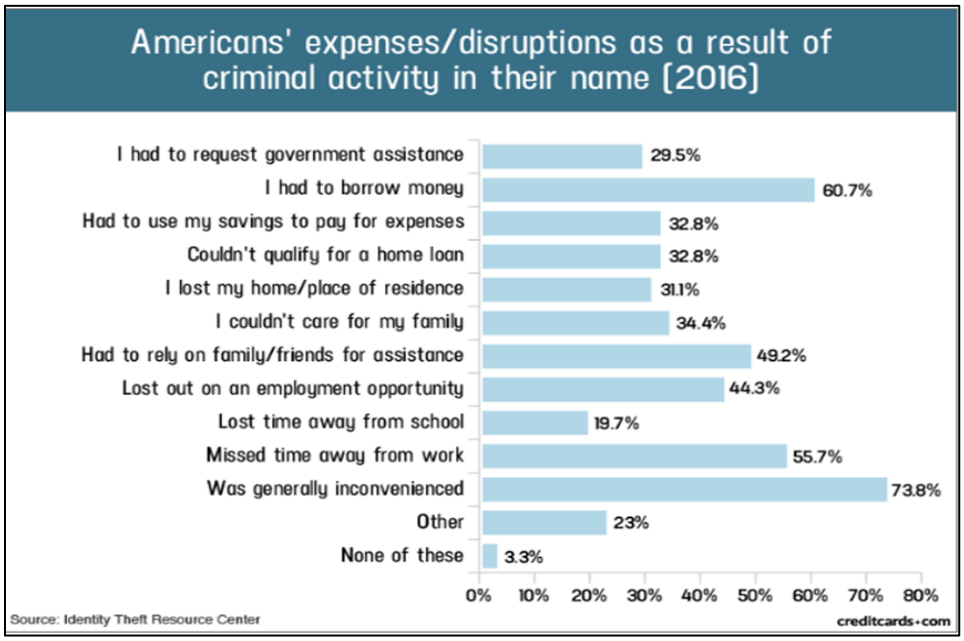
72. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

73. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiff's PII impairs their ability to participate in the economic marketplace.

[12] *See* https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on Feb. 9, 2024).

[13] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

74. A study by the Identity Theft Resource Center[14] shows the multitude of harms caused by fraudulent use of PII:



75. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[15]

> [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.

[14] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited Feb. 9, 2024).

[15] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Feb. 9, 2024).

76. 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.

77. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

G. Plaintiff's and Class Members' Damages

Plaintiff Esther Hicks's Experience

78. When Plaintiff Hicks first became a customer, Defendants required Plaintiff Hicks provide them with substantial amounts of her PII.

79. On or about January 26, 2024, Plaintiff Hicks received a letter entitled "Notice of Data Breach" which told her that her Private Information had been affected during the Data Breach. The notice letter informed her that the Private Information compromised included her "name, Social Security number, date of birth, and policy number(s)."

80. The notice letter offered Plaintiff Hicks only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Hicks will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her Private Information.

81. Plaintiff Hicks suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

82. Plaintiff Hicks would not have provided her Private Information to Defendants had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard their customers' personal information from theft, and that those systems were subject to a data breach.

83. Plaintiff Hicks suffered actual injury in the form of having her Private Information compromised and/or stolen as a result of the Data Breach.

84. Plaintiff Hicks suffered actual injury in the form of damages to and diminution in the value of her personal information – a form of intangible property that Plaintiff Hicks entrusted to Defendants for the purpose of receiving life insurance related services from Defendants which was compromised in, and as a result of, the Data Breach.

85. Plaintiff Hicks suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

86. Plaintiff Hicks has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendants, is protected and safeguarded from future breaches.

87. As a result of the Data Breach, Plaintiff Hicks made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendants, as well as long-term credit monitoring options she will now need to use. Plaintiff Hicks has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

88. As a result of the Data Breach, Plaintiff Hicks has suffered anxiety as a result of the release of her Private Information to cybercriminals, which Private Information she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of committing cyber and other crimes against her. Plaintiff Hicks is very concerned about this

increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on her life.

89. Plaintiff Hicks also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of her Private Information, a form of property that Defendants obtained from Plaintiff Hicks; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

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

91. In sum, Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

92. Plaintiff and Class Members entrusted their Private Information to Defendants in order to receive Defendants' services.

93. Plaintiff's Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendants' inadequate data security practices.

94. As a direct and proximate result of Defendants' actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, loans opened in their names, tax returns and insurance claims filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

95. Further, as a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

96. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

97. The Private Information maintained by and stolen from Defendants' systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

98. Plaintiff and Class Members also lost the benefit of the bargain they made with Defendants. Plaintiff and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiff and Class Members paid to Defendants was intended to be used by Defendants to fund adequate security of their network and systems and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class did not receive what they paid for.

99. Additionally, as a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

100. 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.

101. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII and PHI 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. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[16] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[17]

102. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

103. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. The contractual bargain entered into between Plaintiff and Defendants included

[16] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on Feb. 9, 2024).

[17] *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Feb. 9, 2024).

Defendants' contractual obligation to provide adequate data security, which Defendants failed to provide. Thus, Plaintiff and Class Members did not get what they bargained for.

104. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach 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. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

c. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

105. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Defendants, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

106. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

107. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

108. Specifically, Plaintiff proposes the following Nationwide Class, as well as the following California Subclass definition (also collectively referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.
>
> **California Subclass**
>
> All residents of California who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

109. Excluded from the Class are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

110. Plaintiff reserves the right to modify or amend the definitions of the proposed Nationwide Class, as well as the California Subclass before the Court determines whether certification is appropriate.

111. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

112. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of over 66,000 customers of CNO and its subsidiaries whose data was compromised in the Data Breach. The identities of Class Members

are ascertainable through Defendants' records, Class Members' records, publication notice, self-identification, and other means.

113. 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 engaged in the conduct alleged herein;

b. Whether Defendants' conduct violated the statutes invoked below;

c. When Defendants learned of the Data Breach;

d. Whether Defendants' response to the Data Breach was adequate;

e. Whether Defendants unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

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

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

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

i. Whether Defendants owed a duty to Class Members to safeguard their Private Information;

j. Whether Defendants breached their duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

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

o. What damages Plaintiff and Class Members suffered as a result of Defendants' misconduct;

p. Whether Defendants' conduct was negligent;

q. Whether Defendants' conduct was *per se* negligent;

r. Whether Defendants were unjustly enriched;

s. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

u. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

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

115. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

116. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated 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.

117. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. 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, conducting 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.

118. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendants have acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

119. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class)

120. Plaintiff restates and realleges all of the allegations stated above and hereafter as if fully set forth herein.

121. Defendants knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

122. Defendants knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. Defendants were on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

123. Defendants owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. Defendants' duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the FTCA and California consumer laws;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

124. Defendants' duty to employ reasonable data security measures arose, in part, 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.

125. Defendants' duty also arose because Defendants were bound by industry standards to protect their customers' confidential Private Information.

126. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendants, and Defendants owed them a duty of care to not subject them to an unreasonable risk of harm.

127. Defendants, through their actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendants' possession.

128. Defendants, by their actions and/or omissions, breached their duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

129. Defendants, by their actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

130. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. 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' Private Information;

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

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information; and

e. Failing to comply with the FTCA.

131. Defendants had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Defendants with their Private Information was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems (and the Private Information that they stored on them) from attack.

132. Defendants' breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

133. As a result of Defendants' ongoing failure to notify Plaintiff and Class Members regarding exactly what Private Information has been compromised, Plaintiff and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

134. Defendants' breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

135. As a result of Defendants' negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

136. Defendants also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

137. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

138. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

139. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

140. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen its data security systems and

monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and the Nationwide Class)

141. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

142. Pursuant to Section 5 of the FTCA, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

143. Defendants breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

144. Plaintiff and Class Members are within the class of persons that the FTCA is intended to protect.

145. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Defendants' duty in this regard.

146. Defendants violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

147. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Defendants' networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

148. Defendants' violations of the FTCA constitute negligence *per se*.

149. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to Defendants' negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

150. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

151. Defendants breached their duties to Plaintiff and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

152. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

153. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF CONTRACT
(On behalf of Plaintiff and the Nationwide Class)

154. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

155. Plaintiff and Class Members entered into a valid and enforceable contract through which they paid money to Defendants in exchange for services. That contract included promises by Defendants to secure, safeguard, and not disclose Plaintiff's and Class Members' Private Information.

156. Washington National's Privacy Policy memorialized the rights and obligations of Defendants and their customers. This document was provided to Plaintiff and Class Members in a manner in which it became part of the agreement for services.

157. In their Privacy Policy, Defendants commit to protecting the privacy and security of their customers' Private Information.

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

159. However, Defendants did not secure, safeguard, and/or keep private Plaintiff's and Class Members' Private Information, and therefore Defendants breached their contracts with Plaintiff and Class Members.

160. Defendants allowed third parties to access, copy, and/or exfiltrate Plaintiff's and Class Members' Private Information without permission. Therefore, Defendants breached the Privacy Policy with Plaintiff and Class Members.

161. Defendants' failure to satisfy their confidentiality and privacy obligations resulted in Defendants providing services to Plaintiff and Class Members that were of a diminished value.

162. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendants' failure to fully perform their part of the bargain with Plaintiff and Class Members.

163. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

164. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class)

165. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

166. This Count is pleaded in the alternative to Count III above.

167. CNO, through its subsidiary, Washington National, provides health and life insurance to Plaintiff and Class Members. Plaintiff and Class Members formed an implied contract with Defendants regarding the provision of those services through their collective conduct, including by Plaintiff and Class Members paying for goods and services from Defendants.

168. Through Defendants' sale of health and life insurance products and services, it knew or should have known that it must protect Plaintiff's and Class Members' confidential Private Information in accordance with their policies, practices, and applicable law.

169. As consideration, Plaintiff and Class Members paid money to Defendants and turned over valuable Private Information to Defendants. Accordingly, Plaintiff and Class Members bargained with Defendants to securely maintain and store their Private Information.

170. Defendants accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing insurance products and services to Plaintiff and Class Members.

171. In delivering their Private Information to Defendants and paying for such products and services, Plaintiff and Class Members intended and understood that Defendants would adequately safeguard the Private Information as part of that service.

172. Defendants' implied promises to Plaintiff and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of their employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

173. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of such an implied contract.

174. Had Defendants disclosed to Plaintiff and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and Class Members would not have provided their Private Information to Defendants.

175. Defendants recognized that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

176. Defendants violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Private Information.

177. Plaintiff and Class Members have been damaged by Defendants' conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT V
VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT
CAL. CIV. CODE 1798.100, ET SEQ.
(On behalf of Plaintiff and the California Subclass)

178. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as if fully set forth herein.

179. Plaintiff and California Subclass Members are residents of California.

180. Defendants are corporations organized or operated for the profit or financial benefit of their owners. Defendants collect consumers' personal information (for the purposes of this section, "Private Information") as defined in the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.140.

181. Defendants violated § 1798.150 of the CCPA by failing to prevent Plaintiff's and California Subclass Members' nonencrypted Private Information from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

182. Defendants have a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff's and California Subclass Members' Private Information. As detailed herein, Defendants failed to do so.

183. As a direct and proximate result of Defendants' acts, Plaintiff's and California Subclass Members' Private Information, including names, Social Security numbers, date of birth, and policy number(s) were subjected to unauthorized access and exfiltration, theft, or disclosure.

184. Plaintiff and California Subclass Members seek injunctive or other equitable relief to ensure Defendants hereinafter properly safeguards customer Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continues to hold customer Private Information, including Plaintiff's and California Subclass Members' Private Information. Plaintiff and California Subclass Members have an interest in ensuring that their Private Information is reasonably protected.

185. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendants and third parties with similar inadequate security measures.

186. Plaintiff and the California Subclass seek actual damages, as well as all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorneys' fees and costs.

187. Plaintiff intends to provide Defendants with written notice of their violations of the CCPA, pursuant to Cal. Civil Code § 1798.150(b)(1), asserting violations of Cal. Civil Code §§ 1798.81.5 and 1798.150.

188. If Washington National has not cured or is unable to cure the violations described therein within thirty days of receipt of such notice, Plaintiff will amend her complaint to seek all relief available under the CCPA, including damages to be measured as the greater of actual damages or statutory damages in an amount up to $750.00 per consumer per incident. See Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

189. As a result of Defendants' failure to implement and maintain reasonable data security procedures and practices that resulted in the Data Breach, Plaintiff and the California Subclass seek injunctive relief, including public injunctive relief and declaratory relief.

COUNT VI
VIOLATION OF CALIFORNIA UNFAIR COMPETITION ACT
CAL. BUS. & PROF. CODE 17200, *ET SEQ.*
(On behalf of Plaintiff and the California Subclass)

190. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as if fully set forth herein.

191. Defendants are "person[s]" as defined by Cal. Bus. & Prof. Code § 17201.

192. Defendants violated Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

193. Defendants' "unfair" acts and practices include:

a. Failure to implement and maintain reasonable security measures to protect Plaintiff's and California Subclass Members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Failure to identify foreseeable security risks, remediate identified security risks, and sufficiently improve security following previous cybersecurity incidents, as described herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and California Subclass Members, whose Private Information has been compromised;

c. Failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These

policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100;

d. Failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not have known of Washington National's grossly inadequate security, consumers could not have reasonably avoided the harms that Washington National caused; and

e. Engagement in unlawful business practices by violating Cal. Civ. Code § 1798.82.

194. Defendants has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), the FTC Act, 15 U.S.C. § 45, and California common law.

195. Defendants' unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' Private Information,

including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and California Subclass Members' Private Information;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, and California's Customer Records Act, Cal. Civ. Code § 1798.80, et seq., and § 1798.81.5, which was a direct and proximate cause of the Data Breach; and

h. Failing to provide the Notice of Data Breach required by Cal. Civ. Code § 1798.82(d)(1).

196. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

197. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass Members were injured and suffered monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendants' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

198. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California Subclass Members' rights.

199. Plaintiff and California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

200. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

201. On behalf of herself and other members of the Class, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover actual damages, and reasonable attorneys' fees.

COUNT VII
VIOLATION OF CALIFORNIA CONSUMER LEGAL REMEDIES ACT
CAL. CIV. CODE §§ 1750, ET SEQ.
(On behalf of Plaintiff and the California Subclass)

202. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs as if fully set forth herein.

203. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, et seq. ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

204. Defendants are "person[s]" as defined by Civil Code §§ 1761(c) and 1770 and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

205. Plaintiff and the California Subclass are "consumers" as defined by Civil Code §§ 1761(d) and 1770 and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

206. Defendants' acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass Members in violation of Civil Code § 1770, including by:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

207. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

208. Had Defendants disclosed to Plaintiff and California Subclass Members that their data systems were not secure and, thus, were vulnerable to attack, Defendants would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendants was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff and California Subclass Members. Defendants accepted the responsibility of protecting the data but kept the inadequate state of their security controls secret from the public. Accordingly, Plaintiff and California Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

209. As a direct and proximate result of Defendants' violations of California Civil Code § 1770, Plaintiff and California Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendants' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

210. Plaintiff and the California Subclass seek injunctive relief, including an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA. Pursuant to Cal. Civ. Code § 1782(a), Plaintiff will serve Defendants with notice of their alleged

violations of the CLRA by certified mail return receipt requested. If, within thirty days after the date of such notification, Defendants fail to provide appropriate relief for their violations of the CLRA, Plaintiff will amend this Complaint to seek damages.

COUNT VIII
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class)

211. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

212. This Count is pleaded in the alternative to Counts III and IV above.

213. Plaintiff and Class Members conferred a benefit on Defendants by turning over their Private Information to Defendants and by paying for products and services that should have included cybersecurity protection to protect their Private Information. Plaintiff and Class Members did not receive such protection.

214. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including from payments made to them by Plaintiff and Class Members.

215. As such, a portion of the payments made by Plaintiff and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Washington National.

216. Defendants have retained the benefits of their unlawful conduct, including the amounts of payment received from Plaintiff and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

217. Defendants knew that Plaintiff and Class Members conferred a benefit upon it, which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiff's and Class Members' Private Information and prevented the Data Breach.

218. If Plaintiff and Class Members had known that Defendants had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendants.

219. Due to Defendants' conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendants to be permitted to retain the benefit of their wrongful conduct.

220. 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) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) 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; (v) the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vi) future costs in terms of time, effort, and money that will be

expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

221. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

222. Plaintiff and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IX
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Nationwide Class)

223. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

224. 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 that are tortious and violate the terms of the federal and state statutes described in this Complaint.

225. Defendants owe a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

226. Defendants still possess Private Information regarding Plaintiff and Class Members.

227. Plaintiff alleges that Defendants' data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her Private

Information and the risk remains that further compromises of her Private Information will occur in the future.

228. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure their customers' Private Information and to timely notify customers of a data breach under the common law and Section 5 of the FTCA;

b. Defendants' existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect customers' Private Information; and

c. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure customers' Private Information.

229. This Court should also issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with legal and industry standards to protect customers' Private Information, including the following:

a. Order Defendants to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendants' explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and

ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training their security personnel regarding any new or modified procedures;

iv. segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating their customers about the threats they face with regard to the security of their Private Information, as well as the steps Defendants' customers should take to protect themselves.

230. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If another breach of Defendants' network occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

231. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Plaintiff will likely be subjected to substantial, continued

identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendants' compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

232. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Defendants, thus preventing future injury to Plaintiff and other customers whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Classes described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Classes as requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiff is a proper representative of the Nationwide Class and the California Subclass requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendants to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Defendants to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: February 9, 2024

Respectfully submitted,

/s/ Mason A. Barney
Mason A. Barney
Tyler J. Bean (*pro hac vice* forthcoming)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: tbean@sirillp.com

ClassAction.org
