UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

IN RE: FORTRA FILE TRANSFER SOFTWARE DATA SECURITY BREACH LITIGATION **This Document Relates to: Track Three**	Case No. 24-md-03090-RAR MDL No. 3090

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Cindy Rougeau, Beverly Banks, Mark Brewer, Randall Carter, Tammy Eddie, Nigel Keep, Vincentina Luciano, David Mueller, Jeanne Peffley-Wilson, Roberta Platt, Michelle Ronne, Anthony Tetreault, Gordon Titcomb, Roderick Veazey, Nicholas Venezia, Valarie Venezia, Donna Vogel, John Vogel, Ariana Skurauskis, Renee Rogers, Noah Rogers, Arnisha Shepherd Shontay Marhsall (collectively "Plaintiffs"), individually and on behalf of all others similarly situated, assert the following against Defendants Aetna Inc. and Aetna Life Insurance Company (collectively, "Aetna"), Santa Clara Family Health Plan ("SCFHP"), Anthem Insurance Companies, Inc. d/b/a Anthem Blue Cross and Blue Sheild ("Anthem" or "BCBS"), and Elevance Health, Inc. ("Elevance") (collectively "Defendants") based on Plaintiffs' personal knowledge, investigation of counsel, facts of public record, and information and belief as to all other matters.

I. NATURE OF THE ACTION

1. This class action arises out of Defendants' abdication of the myriad legal and equitable duties they owe millions of patients and customers to safeguard their sensitive, Personally Identifiable Information ("PII") and Protected Health Information[1] ("PHI") (collectively, PII and PHI are referred to as "Personal Information").

[1] PHI includes PII.

2. Like all patients and customers in the United States, Plaintiffs and Class Members (defined herein) entrusted their PII and PHI to Defendants and permitted Defendants to gather their PII and PHI in connection with the treatment, products, and healthcare and other related services Plaintiffs and the Class Members purchased or received from Defendants. This entrustment was made in confidence with the reasonable expectation – indeed, obligation – Defendants would fulfill their duties and obligations to safeguard Plaintiffs' and the Class Members' Personal Information.

3. Plaintiffs and Class Members expected Defendants to comply with federal and state law and to, *inter alia*, implement and execute safeguards that would ensure that: (a) Defendants' patients' and customers' PII and PHI is stored and transmitted securely; (b) Defendants would only share patient and customer PII and PHI when necessary and in compliance with their policies and procedures and the law; (c) Defendants would notify patients and customers promptly if their information was compromised due to, among other things, unauthorized access; and, (d) Defendants would comply with the law and provide adequate mitigation to the Plaintiffs and Class Members for the harm suffered as a result of the wrongful disclosure of their PHI and PII.

4. Defendants failed to fulfil their basic legal duties and obligations. And because of Defendants' failures, between January 30 and February 7, 2023, unauthorized third parties gained access to the PII and PHI of millions of Defendants' patients and customers, including their names, genders, health plan subscriber numbers, Medicare numbers, addresses, phone numbers, dates of birth, treatment information, diagnosis, patient account numbers, medical ID numbers, health insurance information, and prescription information (the "Data Breach" or "Breach").[2] This data is recognized as valuable by many different constituencies, including (1) Defendants themselves, (2) the cybercriminals who exfiltrated the PII and PHI for purposes of selling it to others who

[2] https://apps.web.maine.gov/online/aeviewer/ME/40/0461b276-a513-41ae-a587-c06c971a7d9b.shtml.

intend to commit identity and medical theft and fraud, and (3) Plaintiffs and Class Members, whose PII and PHI was stolen.

5. Upon information and belief, Defendants used a third party-vendor, NationsBenefits, to provide additional services to Defendants' patients and customers. Defendants are "Covered Entities" and NationsBenefits was Defendants' "Business Associate," as those terms are defined under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

6. NationsBenefits used the vendor Fortra, LLC ("Fortra") for information technology management and software services, including Fortra's file-transfer platform, GoAnywhere MFT.

7. Pursuant to Business Associate Agreements between NationsBenefits and Defendants, each Defendant affirmatively transferred the PII and PHI of millions of Defendants' patients and customers to NationsBenefits despite the fact that the overwhelming majority of Class Members did not use the services NationsBenefits provides and likely never would. In fact, prior to this Breach, *many Plaintiffs and Class Members were not aware of the existence of NationsBenefits, let alone the fact that NationsBenefits possessed their PII and PHI.* As such, NationsBenefits was not authorized to obtain Plaintiffs' and Class Members' PII and PHI from any of the Defendants, and Defendants had no legitimate business reason to provide Plaintiffs' and Class Members' PII and PHI to NationsBenefits; yet Defendants did so affirmatively without authorization, consent, or legitimate business need.

8. On or about January 30, 2023, an unauthorized party gained access to Plaintiffs' and Class Members' PII and PHI by accessing the servers of NationsBenefits in the Data Breach."

9. Upon information and belief, the unauthorized third-party that perpetrated the Data Breach are cybercriminals part of a Russian-linked hacker/ransomware group, Clop, responsible

for numerous other hacking events of which Defendants were surely aware.[3] Upon information and belief, Clop perpetrated the Data Breach for the purpose of engaging in identity theft to the detriment and injury of Plaintiffs and Class Members. Upon further information and belief, Clop has already begun to leak Plaintiffs' and Class Members' Personal Information.[4]

10. Exacerbating the harm the Data Breach caused, Plaintiffs and Class Members were not informed of the Data Breach for months after it occurred.

11. On February 1, 2023, Fortra, LLC disclosed to its customers, including NationsBenefits, that its file transfer platform, GoAnywhere MFT, had been hacked, resulting in the exfiltration of customer PII and PHI, including Plaintiff's and Class Members PII and PHI.

12. In April 2023, NationsBenefits began a rolling notice of the Data Breach to Defendants' patients and customers.

13. In or around the same time, SCFHP sent notice of the Data Breach to its customers.

14. To date, Aetna, Anthem and Elevance have never provided their customers, including the Aetna, Anthem and Elevance Plaintiffs, with direct notice of the Data Breach, despite Aetna's, Anthem's, and Elevance's Defendants' own statutory and regulatory obligations to do so.

15. The letter to Plaintiffs and Class Members from NationsBenefits stated that the Personal Information accessed or acquired by the malicious actor(s) included Plaintiffs' and Class

---

[3] https://www.scmagazine.com/news/ransomware/clop-ransomware-hack-of-fortra-goanywhere-mft-hits-1m-chs-patients; https://www.aha.org/news/headline/2023-02-23-hhs-russia-linked-ransomware-group-claims-continued-health-care-attacks. Indeed, most health insurance companies are members of trade associations, such as Health-ISAC, which monitor and share information with other healthcare entities regarding past and ongoing threats to information security. "Health-ISAC" stands for Health Information Sharing and Analysis Center and "is primarily focused on sharing timely, actionable and relevant information with each other including intelligence on threats, incidents and vulnerabilities that can include data such as indicators of compromise, tactics, techniques and procedures (TTPs) of threat actors, advice and best practices, mitigation strategies and other valuable material.." *See About*, HEALTH-ISAC, https://h-isac.org/about-h-isac/.

[4] https://www.bleepingcomputer.com/news/security/clop-now-leaks-data-stolen-in-moveit-attacks-on-clearweb-sites/.

Members' first name, last health plan subscriber number, gender, Social Security number, address, phone number, and date of birth.

16. Recognizing the possibility of identity theft to Plaintiffs and Class Members, both present and future, NationsBenefits offered two years of credit monitoring through Experian Identityworks.

17. Upon information and belief, Clop has already posted and/or sold Plaintiffs' and Class Members' Personal Information on their dark web-based store, known as "Clop Leaks."[5]

18. In a statement, the hackers claimed that they could access other parts of victim's networks and systems and deploy malware, "but decided against it and only stole the documents stored on the compromised GoAnywhere MFT servers."[6]

19. Upon information and belief, other cybercriminal groups and attackers leveraged this exploitation alongside Clop.[7]

20. Upon information and belief, NationsBenefits and Fortra left Plaintiffs' and Class Members' Personal Information accessible, unprotected, unencrypted, and therefore easily accessible for unauthorized access and exfiltration.

21. Each Defendant has a duty to safeguard and protect health plan member information entrusted to it and could have prevented this theft had it limited the customer information it shared with its business associates and employed reasonable measures to ensure its

---

[5] *Id.*

[6] Sergui Gatlan, *Clop ransomware claims it breached 130 orgs using GoAnywhere zero-day*, BLEEPINGCOMPUTER (Feb. 10, 2023), https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day.

[7] Ido Lev, *BlackCat / Alphv Ransomware Group Exploits GoAnywhere Vulnerability (CVE-2023-0669) With Higher-Than-Average Demands*, AT BAY (Apr. 25, 2023), https://www.at-bay.com/articles/blackcat-ransomware-group-exploits-goanywhere-vulnerability.

business associates such as NationsBenefits implemented and maintained adequate data security measures and protocols in order to secure and Aetna customers' and policyholders' data.

22. Upon information and belief, prior to and through the date of the Data Breach, each Defendant obtained Plaintiffs' and Class Members' PII and PHI, maintained that sensitive data in a negligent and/or reckless manner, and failed to prevent its business associates such as NationsBenefits from doing the same.

23. File transfer services like GoAnywhere MFT are popular and well-known targets for cyberattacks. Some of the largest healthcare data breaches in recent history occurred by cyber criminals targeting file transfer services. For example, in February 2021, the file transfer service Accellion was attacked by the same threat actors as the Data Breach (Clop), causing the theft of more than three million patients' and customers' information.[8]

24. Defendants knew or should have known, including through membership in trade associations like Health-ISAC, that services from third-party vendors like Fortra were frequently attacked, leading to ninety percent of healthcare-related cyberattacks in 2021 and 2022.[9]

25. The frequency and prevalence of these attacks make it imperative for entities like Defendants to monitor for exploits and attacks routinely and constantly, and regularly update their software, security, and monitoring procedures.

---

[8] Ionut Ilascu, *Global Accellion data breaches linked to Clop ransomware gang,* BLEEPINGCOMPUTER (Feb. 22, 2021), https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/; *Exploitation of Accellion File Transfer Appliance*, CYBERSECURITY INFRASTRUCTURE & SECURITY AGENCY (June 17, 2021), https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-055a.

[9] Jessica Davis, *Most of the 10 largest healthcare data breaches in 2022 are tied to vendors*, SC MEDIA (Dec. 12, 2022), https://www.scmagazine.com/feature/breach/most-of-the-10-largest-healthcare-data-breaches-in-2022-are-tied-to-vendors; Jessica Davis, *Vendor incidents lead the 10 biggest health care data breaches of 2021 so far*, SC MEDIA (June 30, 2021), https://www.scmagazine.com/news/risk-management/vendor-incidents-lead-the-10-biggest-health-care-data-breaches-of-2021-so-far.

26. Defendants were fully aware that the healthcare benefits industry is a prime target for cyber threats.[10] High profile data breaches in for similar industry leaders in healthcare put them on notice of this fact, *e.g.*, Trinity Health (3.3 million patients, May 2020); Shields Healthcare Group (2 million patients, March 2022). Between 2020 and 2021, attacks on the healthcare industry increased 71%, making it the fifth most common industry targeted by cyberattacks.[11]

27. Defendants also knew or should have known of the threat that Clop posed to their patients and customers. The healthcare industry is the primary target of Clop.[12] Moreover, the U.S. Department of Health and Human Services issued alerts in 2021 and early January 2023 warning the healthcare sector of potential Clop attacks.[13] Clop has previously targeted file transfer services as a means to target the healthcare sector.[14]

28. Armed with the PII and PHI stolen in the Data Breach, criminals can commit a litany of crimes. Specifically, criminals can now open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' health information to craft phishing and other hacking attacks based on Class Members' individual health needs, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

---

[10] *See* Finkle, *FBI warns healthcare firms they are targeted by hackers*, *supra* n.3.
[11] Check Point Research Team, *Check Point Research: Cyber Attacks Increased 50% Year over Year*, Check Point (Jan. 10, 2022), https://blog.checkpoint.com/security/check-point-research-cyber-attacks-increased-50-year-over-year.
[12] HC3, *Analyst Note: Clop Ransomware*, HHS (Jan. 4, 2023), https://www.hhs.gov/sites/default/files/clop-ransomware-analyst-note-tlpclear.pdf.
[13] *Id*.
[14] HC3, *Analyst Note: CLOP Poses Ongoing Risk to HPH Organizations*, HHS (Mar. 23, 2021), https://www.hhs.gov/sites/default/files/clop-poses-ongoing-risk-to-hph-organizations.pdf.

29. As a result of each Defendant's negligent and/or reckless conduct and affirmative acts, Plaintiffs and Class Members now suffer from a heightened and imminent risk of fraud and identity theft and must constantly monitor their financial accounts. Plaintiffs and Class Members also will likely suffer additional financial costs for purchasing necessary credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

30. Plaintiffs and Class Members have suffered—and will continue to suffer—from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or diminished value of their PII and PHI, the value of their time reasonably incurred to mitigate the fallout of the Data Breach, nominal damages, and are under a current and continuous threat of having their PII and PHI exploited to their detriment for gain by cybercriminals.

31. Plaintiffs thus bring this class action against Defendants for the injuries inflicted on Plaintiffs and millions[15] of similarly situated persons ("Class Members") due to Defendants' (a) failure to properly secure and safeguard highly valuable, PII and PHI, including without limitation, names, addresses, emails, phone numbers, health plan account and ID numbers, dates of birth, and Medicare numbers; (b) failure to comply with industry standards to protect information systems that contain PII and PHI or otherwise ensure that their HIPAA business associate complied with such standards; (c) failure to comply with Defendants' own policies and procedures for the protection of PHI and PII; (d) unlawful, affirmative disclosure of the PII and PHI of Plaintiffs and Class Members to NationsBenefits who was not authorized or had no legitimate business need to receive that information; (e) failure to take affirmative action following the Data Breach to reobtain and secure the PHI and PII, investigate the incident, take affirmative steps to remediate Defendants

[15] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf .

systems and protect against further disclosure, and mitigate the harm caused to the patients and customers; and (f) failure to provide adequate notice to Plaintiffs and Class Members that their PII and PHI had been disclosed and compromised.

32. Plaintiffs, on behalf of themselves and all others similarly situated, bring claims for negligence, negligence *per se*, breach of contract, breach of implied contract, unjust enrichment, breach of fiduciary duty of confidentiality, declaratory judgment, violations of consumer protection statutes of their home states, violations of data protection and consumer privacy statutes of their home states, and injunctive relief.

33. Plaintiffs seek remedies including, but not limited to, compensatory damages, treble damages, nominal damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief requiring Defendants to, *inter alia*, (a) adopt reasonably sufficient practices to safeguard the PII and PHI in Defendants' and Defendants' business associates' custody and control; and (b) to properly evaluate, oversee, and monitor data in the custody of business associates hired by Defendants to prevent incidents like the Data Breach from recurring more thoroughly properly and adequately.

34. Given that information relating to the Data Breach remains exclusively in Defendants' and NationsBenefits' control, Plaintiffs anticipate that additional information in support for their claims will emerge during discovery.

II. JURISDICTION AND VENUE

35. This Court has original jurisdiction under the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2), because the amount in controversy for the Class exceeds the sum of $5,000,000, exclusive of interest and costs, there are more than 100 Class Members, and

minimal diversity exists because many Plaintiffs and many Class Members are citizens of a different state than Defendants.

36. This Court has general and specific personal jurisdiction over each Defendant because Defendants either conduct substantial business and other activities in this jurisdiction or have been transferred to this Court through consolidation by the Judicial Panel on Multidistrict Litigation.

37. Venue is proper in this District either under 28 U.S.C. §§ 1391(b) because a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendants conducts substantial business in this District, or under 28 U.S.C. § 1407, because the underlying cases have been transferred to this Court through consolidation by the Judicial Panel on Multidistrict Litigation.

III. PARTIES

A. Plaintiffs

Plaintiff Cindy Rougeau

38. Plaintiff Cindy Rougeau ("Plaintiff Rougeau") is a citizen and resident of New York.

39. Plaintiff Rougeau has maintained health insurance coverage through Aetna. Aetna required Plaintiff Rougeau to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Rougeau's PII and PHI to NationsBenefits after she enrolled with Aetna.

40. Plaintiff Rougeau received a letter dated April 27, 2023, notifying Plaintiff Rougeau that as an insured customer of Aetna her first name, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were

compromised in the Data Breach.

41. Shortly after and as a result of the Data Breach, Plaintiff Rougeau was the victim of fraud and identity theft. Specifically, she experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers where she was asked to provide personal information, join alleged social media groups, or click on weblinks. In addition, she received a call from Target regarding a credit card she purportedly opened, although Plaintiff Rougeau never had applied for such a credit card. An unidentified charge for apparel from a concert in Jones Beach, New York also appeared on Plaintiff Rougeau's credit card statement shortly after the Data Breach, even though she never has visited Jones Beach. Plaintiff Rougeau also received a letter from a likely fraudster claiming to be the IRS seeking to obtain Plaintiff Rougeau's personal information. Similarly, Plaintiff became aware that hackers had unsuccessfully tried to gain access to her email account approximately 93 times. Indeed, Equifax recently informed Plaintiff Rougeau that her confidential information is on the dark web. Aetna even contacted Plaintiff Rougeau about apparent unauthorized attempts to receive medication using Plaintiff Rougeau's name through doctors that Plaintiff Rougeau has never seen as a patient.

42. As a result of the Data Breach and as recommended in the Notice, Plaintiff Rougeau made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, obtaining her credit report from the credit reporting agencies, freezing her credit, signing up for credit monitoring, and continually monitoring her credit information. Plaintiff Rougeau has spent significant time, approximately 50 hours to date, responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff Rougeau suffered lost time,

annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns regarding the loss of her privacy over the impact of cybercriminals accessing and using her PII and PHI.

43. Plaintiff Rougeau reviewed and agreed to Aetna's privacy policies in mailings she received from Aetna. Plaintiff Rougeau believed and reasonably expected that Aetna would protect her PII and PHI once she provided it to Aetna. Plaintiff Rougeau would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI.

44. Thus, as a result of the Data Breach, Plaintiff Rougeau has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Rougeau has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff Beverly Banks

45. Plaintiff Beverly Banks ("Plaintiff Banks") is a citizen and resident of Michigan.

46. Plaintiff Banks has maintained health insurance coverage through Aetna. Aetna required Plaintiff Banks to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Banks's PII and PHI to NationsBenefits after she enrolled with Aetna.

47. Plaintiff Banks received a letter dated April 27, 2023, notifying Plaintiff Banks that as an insured customer of Aetna her first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

48. Shortly after and as a result of the Data Breach, Plaintiff Banks was the victim of

fraud and identity theft. Specifically, she experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers where she is asked to provide personal information, press a number to continue, or click on weblinks, resulting in her need to shut her phone off. In addition, she received an alert through her Experian account regarding an "account inquiry" or "credit card inquiry," which she did not request. Indeed, Equifax recently informed Plaintiff Banks that her confidential information is on the dark web.

49. As a result of the Data Breach and as recommended in the Notice, Plaintiff Banks made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, calling Aetna and/or NationsBenefits regarding more information about this Data Breach, and continually monitoring her credit information. Plaintiff Banks has spent significant time, approximately 11 hours to date, responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work or recreation. Plaintiff Banks suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy..

50. Plaintiff Banks does not recall receiving, reviewing, or agreeing to Aetna's privacy policies in mailings from Aetna. Plaintiff Banks reasonably believed that Aetna would protect her PII and PHI once she provided it to Aetna. Plaintiff Banks would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI.

51. Thus, as a result of the Data Breach, Plaintiff Banks has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Banks has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future

data breaches.

Plaintiff Mark Brewer

52. Plaintiff Mark Brewer ("Plaintiff Brewer") is a citizen and resident of Oklahoma.

53. Plaintiff Brewer has maintained health insurance coverage through Aetna. Aetna required Plaintiff Brewer to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Brewer's PII and PHI to NationsBenefits after he enrolled with Aetna.

54. Plaintiff Brewer received a letter dated April 27, 2023, notifying Plaintiff Brewer that as an insured customer of Aetna his first name, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

55. Shortly after and as a result of the Data Breach, Plaintiff Brewer was the victim of fraud and attempted identity theft. Specifically, he experienced a large increase in spam phone calls and suspicious text messages from strangers trying to solicit a response, as well as someone posing as a representative of United Health asking for sensitive personal information after he signed up for his new insurance plan; he confirmed with the real United Health that this was a fraudulent call.

56. As a result of the Data Breach and as recommended in the Notice, Plaintiff Brewer made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, freezing his credit through Equifax, and calling and emailing NationsBenefits and Aetna directly do find out more about the breach. Plaintiff Brewer has spent significant time, including 3-4 hours of phone calls, 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. Plaintiff Brewer suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anger and increased concerns regarding the loss of his privacy and potential further damages over the impact of cybercriminals accessing and using his PII and PHI. Plaintiff Brewer is also concerned that because he lives on a month-to-month check, he likely won't have the time or resources to deal with any potential financial fraud that could occur as a result of the Data Breach. Furthermore, Plaintiff Brewer is upset and concerned that Aetna was not transparent about the third parties they were sharing customers' data with, and the lack of professionalism of the agent who dismissed his requests and laughed at him before directing him to a useless phone number, including a number for a moving company, when he called to speak to Aetna and NationsBenefits about the Data Breach.

57. Plaintiff Brewer reviewed, and agreed to, Aetna's privacy policies with an agent when he first signed up with Aetna. Plaintiff Brewer reasonably believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff Brewer would not have enrolled with Aetna if he had known Aetna would not adequately protect his PII and PHI.

58. Thus, as a result of the Data Breach, Plaintiff Brewer has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Brewer has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff Randall Lynn Carter

59. Plaintiff Randall Lynn Carter ("Plaintiff Carter") is a citizen and resident of Oklahoma.

60. Plaintiff Carter has maintained health insurance coverage through Aetna. Aetna

required Plaintiff Carter to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Carter's PII and PHI to NationsBenefits after he enrolled with Aetna.

61. Plaintiff Carter received a letter dated April 27, 2023, notifying Plaintiff Carter that as an insured customer of Aetna his first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

62. Shortly after and as a result of the Data Breach, Plaintiff Carter was the victim of fraud. Specifically, he experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers, including frequent calls requiring Plaintiff Carter to "press one to continue".

63. As a result of the Data Breach and as recommended in the Notice, Plaintiff Carter made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, obtaining his credit report from the credit reporting agencies, freezing his credit, and continually monitoring his credit information. Plaintiff Carter has spent significant time, including over four hours calling Aetna or NationsBenefits, 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 or recreation. Plaintiff Carter suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of his privacy and the impact of cybercriminals accessing and using his PII and PHI.

64. Plaintiff Carter reviewed and agreed to Aetna's privacy policies in mailings he received from Aetna. Plaintiff Carter believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff Carter would not have enrolled with Aetna if he had known Aetna

would not adequately protect his PII and PHI.

65. Thus, as a result of the Data Breach, Plaintiff Carter has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Carter has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff Tammy Felicia Eddie

66. Plaintiff Tammy Felicia Eddie ("Plaintiff Eddie") is a citizen and resident of North Carolina.

67. Plaintiff Eddie has maintained health insurance coverage through Aetna. Aetna required Plaintiff Eddie to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Eddie's PII and PHI to NationsBenefits after she enrolled with Aetna.

68. Plaintiff Eddie received a letter dated April 27, 2023, notifying Plaintiff Eddie that as an insured customer of Aetna her first name, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

69. Shortly after and as a result of the Data Breach, Plaintiff Eddie was the victim of fraud and identity theft. Specifically, she experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers, sometimes several in a single day, including those asking if she wants to activate her healthy food card – which she already has, and is active, through NationsBenefits, and suspicious charges to some of her accounts. In addition, she has experienced a company called contentbode.com try to make charges to her CashApp application and Direct

Express Card, which she uses for her SSA payments. The attempted CashApp charge was blocked, but Direct Express Card made the requested payments, and only credited her card back when Plaintiff Eddie disputed the unauthorized charges.

70. As a result of the Data Breach and as recommended in the Notice, Plaintiff Eddie made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, monitoring her credit reports through CreditKarma, and discussing what to do next with an attorney. Plaintiff Eddie has spent significant time, approximately 5-10 hours, responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work and/or recreation. Plaintiff Eddie suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy and the impact of cybercriminals accessing and using her PII and PHI.

71. Plaintiff Eddie does not recall receiving, reviewing, or agreeing to Aetna's privacy policies from Aetna or on Aetna's website. Plaintiff Eddie believed that Aetna would protect her PII and PHI once she provided it to Aetna. Plaintiff Eddie would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI.

72. Thus, as a result of the Data Breach, Plaintiff Eddie has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Eddie has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff Nigel Keep

73. Plaintiff Nigel Keep ("Plaintiff Keep") is a citizen and resident of Nevada.

74. Plaintiff Keep has maintained health insurance coverage through Aetna. Aetna required Plaintiff Keep to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Keep's PII and PHI to NationsBenefits after his enrolled with Aetna.

75. Plaintiff Keep received a letter dated April 27, 2023, notifying Plaintiff Keep that as an insured customer of Aetna his first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, and date of birth were compromised in the Data Breach.

76. Shortly after and as a result of the Data Breach, Plaintiff Keep was the victim of fraud and possible attempted identity theft. Specifically, he experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers where he is requested to contact the sender, or to click on a link. In addition, dark web scans indicate some of his information is on the dark web. Plaintiff Keep has kept his credit locked and frozen since the prior Aetna data breach, in 2020.

77. As a result of the Data Breach and as recommended in the Notice, Plaintiff Keep made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, obtaining his credit report from the credit reporting agencies, continually monitoring his credit information, maintains his freeze on his credit accounts, and continues to pay $25 per month for credit monitoring. Despite the credit freeze, Plaintiff Keep continues to monitor his credit and continues to periodically do dark web searches for his information. Plaintiff Keep

has spent significant time, approximately 1-2 hours each month and over two hours on the phone with Aetna or NationsBenefits, 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. Plaintiff Keep suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced a constant "state of vigilance" and concern that his financial security could be destroyed over the impact of cybercriminals accessing and using his PII and PHI. The repeated Aetna data breaches makes Plaintiff Keep feel unsafe.

78. Plaintiff Keep does not recall receiving, reviewing, or agreeing to Aetna's privacy policies from Aetna or on Aetna's website. Plaintiff Keep believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff Keep would not have enrolled with Aetna if he had known Aetna would not adequately protect his PII and PHI.

79. Thus, as a result of the Data Breach, Plaintiff Keep has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Keep has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff Vincentina Luciano

80. Plaintiff Vincentina Luciano ("Plaintiff Luciano") is a citizen and resident of Florida.

81. Plaintiff Luciano has maintained health insurance coverage through Aetna. Aetna required Plaintiff Luciano to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Luciano's PII and PHI to NationsBenefits after she enrolled with Aetna.

82. Plaintiff Luciano received a letter dated April 27, 2023, notifying Plaintiff Luciano that as an insured customer of Aetna her first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, and date of birth were compromised in the Data Breach.

83. Shortly after and as a result of the Data Breach, Plaintiff Luciano was the victim of fraud and identity theft. Specifically, she experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers where she is asked to provide personal information, including a call from someone alleging to be Bank of America, where she did provide personal information. In addition, an unknown party fraudulently accessed her Bank of America account, changed the password, and used Zelle to withdraw money between March and July of 2023. While the money was reimbursed and the account frozen for a time, this incident required her to go to the bank in person to withdraw her funds and ultimately switch banks. An unauthorized person also tried to change her account password with TD Ameritrade (now Charles Schwab), but they were blocked by an alert.

84. As a result of the Data Breach and as recommended in the Notice, Plaintiff Luciano made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, closely reviewing financial and account statements, logging into online accounts to check activity, talking with banks about fraud, freezing her credit, continually monitoring her credit information, and resetting automatic billing instructions and direct deposits. Plaintiff Luciano plans to sign up for credit monitoring, as well. Plaintiff Luciano has spent significant time, approximately 25 hours, responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work or recreation. Plaintiff Luciano suffered lost time, annoyance, interference, and inconvenience as

a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy, including general worry and the bank stating they would deny a loan for home improvements based on the Data Breach, over the impact of cybercriminals accessing and using her PII and PHI.

85. Plaintiff Luciano does not recall receiving, reviewing, or agreeing to Aetna's privacy policies from Aetna or on Aetna's website. Plaintiff Luciano believed that Aetna would protect her PII and PHI once she provided it to Aetna. Plaintiff Luciano would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI.

86. Thus, as a result of the Data Breach, Plaintiff Luciano has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Luciano has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff David Mueller

87. Plaintiff David Mueller ("Plaintiff Mueller") is a citizen and resident of Illinois.

88. Plaintiff Mueller has maintained health insurance coverage through Aetna. Aetna required Plaintiff Mueller to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Mueller's PII and PHI to NationsBenefits after he enrolled with Aetna.

89. Plaintiff Mueller received a letter dated April 27, 2023, notifying Plaintiff Mueller that as an insured customer of Aetna his first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, and date of birth were compromised in the Data Breach.

90. Shortly after and as a result of the Data Breach, Plaintiff Mueller was the victim of fraud and identity theft. Specifically, he experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers asking him to press a number or click a link to continue. In addition, an unauthorized user managed to charge his existing credit card on two separate occasions, resulting in Plaintiff Mueller needing to close a credit card account twice over a two-month period.

91. As a result of the Data Breach and as recommended in the Notice, Plaintiff Mueller made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, constantly monitoring all credit cards, bank accounts, and his PayPal account, maintaining credit monitoring – though Experian didn't catch the fraudulent charges, and maintaining a credit freeze that has been in force for the past three years. Plaintiff Mueller has spent significant time, approximately 35 hours (including 1-2 hours on the phone with Aetna or NationsBenefits), 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 or recreation. Plaintiff Mueller suffered lost time, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of his privacy over the impact of cybercriminals accessing and using his PII and PHI. Indeed, due to the Data Breach, Plaintiff Mueller constantly fears someone will clean out his savings or checking accounts, that his FICO credit score will decrease, that he will suffer home title theft, and will incur more unauthorized charges.

92. Plaintiff Mueller reviewed and agreed to Aetna's privacy policies in mailings he received from Aetna. Plaintiff Mueller believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff Mueller would not have enrolled with Aetna if he had known Aetna

would not adequately protect his PII and PHI.

93. Thus, as a result of the Data Breach, Plaintiff Mueller has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Mueller has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff Jeanne Peffley-Wilson

94. Plaintiff Jeanne Peffley-Wilson ("Plaintiff Peffley-Wilson") is a citizen and resident of Georgia.

95. Plaintiff Peffley-Wilson has maintained health insurance coverage through Aetna. Aetna required Plaintiff Peffley-Wilson to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Peffley-Wilson's PII and PHI to NationsBenefits after she enrolled with Aetna.

96. Plaintiff Peffley-Wilson received a letter dated April 27, 2023, notifying Plaintiff Peffley-Wilson that as an insured customer of Aetna her first name, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

97. Shortly after and as a result of the Data Breach, Plaintiff Peffley-Wilson was the victim of fraud. Specifically, she experienced several scam emails informing her that her various accounts are being closed and she must respond right away or click a link to prevent further action, as well as scam emails posing to be companies such as Amazon. In addition, she received calls and text messages from strangers asking her to press a number to continue, or to click a link because her accounts are past due.

98. As a result of the Data Breach and as recommended in the Notice, Plaintiff Peffley-Wilson made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, making multiple calls to Aetna and NationsBenefits, closely reviewing financial statements, changing the passwords for all of her accounts, and checking her online account statements at least once per week. Plaintiff Peffley-Wilson has spent significant time, approximately 5-6 hours and an additional 1-2 hours each week, responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work or recreation. Plaintiff Peffley-Wilson suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy, including constantly worrying over the impact of cybercriminals accessing and using her PII and PHI.

99. Plaintiff Peffley-Wilson skimmed through and agreed to Aetna's privacy policies when she renewed her policy each year. Plaintiff Peffley-Wilson believed that Aetna would protect her PII and PHI once she provided it to Aetna. Plaintiff Peffley-Wilson would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI.

100. Thus, as a result of the Data Breach, Plaintiff Peffley-Wilson has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Peffley-Wilson has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff Roberta Platt

101. Plaintiff Roberta Platt ("Plaintiff Platt") is a citizen and resident of Massachusetts.

102. Plaintiff Platt has maintained health insurance coverage through Aetna. Aetna

required Plaintiff Platt to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Platt's PII and PHI to NationsBenefits after she enrolled with Aetna.

103. Plaintiff Platt received a letter dated April 27, 2023, notifying Plaintiff Platt that as an insured customer of Aetna her first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, and date of birth, were compromised in the Data Breach.

104. Shortly after and as a result of the Data Breach, Plaintiff Platt was the victim of spam calls and phishing attempts. Specifically, she experienced a large increase in spam and suspicious phone calls, texts, and emails, such as unsolicited credit card offers; Plaintiff Platt doesn't answer the phone for unknown callers, so she is unsure of the nature of most spam calls.

105. As a result of the Data Breach and as recommended in the Notice, Plaintiff Platt made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach, calling Aetna and NationsBenefits on multiple occasions, calling her banks, and monitoring her accounts. Plaintiff Platt has spent significant time, over 5 hours to date, responding to the Data Breach, and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work or recreation. Plaintiff Platt suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and increased concerns regarding the loss of her privacy, including worrying about someone using her name to open credit card accounts or loans using her name, over the impact of cybercriminals accessing and using her PII and PHI.

106. Plaintiff Platt does not recall receiving, reviewing, or agreeing to Aetna's privacy policies from Aetna or Aetna's websites. Plaintiff Platt believed that Aetna would protect her PII

and PHI once she provided it to Aetna. Plaintiff Platt would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI, and is disappointed that Aetna still hasn't contacted its customers directly to inform them of the Data Breach.

107. Thus, as a result of the Data Breach, Plaintiff Platt has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Platt has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff Michelle Ronne

108. Plaintiff Michelle Ronne ("Plaintiff Ronne") is a citizen and resident of North Dakota.

109. Plaintiff Ronne has maintained health insurance coverage through Aetna. Aetna required Plaintiff Ronne to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Ronne's PII and PHI to NationsBenefits after she enrolled with Aetna.

110. Plaintiff Ronne received a letter dated April 27, 2023, notifying Plaintiff Ronne that as an insured customer of Aetna her first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

111. Shortly after and as a result of the Data Breach, Plaintiff Ronne was the victim of fraud and identity theft. Specifically, she experienced a large increase in spam and suspicious phone calls, texts, and emails, such as letters allegedly from the state and from GeekSquad saying Plaintiff Ronne owes them money. As a Result, Plaintiff Ronne no longer answers calls from phone

numbers she does not recognize. In addition, she's had unauthorized purchases attempted with GeekSquad, which her bank is investigating, as well as $238 taken out of her bank account.

112. As a result of the Data Breach and as recommended in the Notice, Plaintiff Ronne made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, obtaining her credit report from the credit reporting agencies, closing and opening new bank accounts, maintaining credit monitoring, and continually monitoring her credit information. Plaintiff Ronne has spent significant time responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work or recreation. Plaintiff Ronne suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy as well as anxiety over the impact of cybercriminals accessing and using her PII and PHI.

113. Plaintiff Ronne reviewed and agreed to Aetna's privacy policies in mailings she received from Aetna. Plaintiff Ronne believed that Aetna would protect her PII and PHI once she provided it to Aetna. Plaintiff Ronne would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI.

114. Thus, as a result of the Data Breach, Plaintiff Ronne has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Ronne has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff Anthony Tetreault

115. Plaintiff Anthony Tetreault ("Plaintiff Tetreault") is a citizen and resident of Kansas.

116. Plaintiff Tetreault has maintained health insurance coverage through Aetna. Aetna required Plaintiff Tetreault to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Tetreault's PII and PHI to NationsBenefits after he enrolled with Aetna.

117. Plaintiff Tetreault received a letter dated April 27, 2023, notifying Plaintiff Tetreault that as an insured customer of Aetna his first name, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

118. Shortly after and as a result of the Data Breach, Plaintiff Tetreault was the victim of fraud and identity theft. Specifically, he experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers and "robocalls", including calls asking him to press a number to continue. In addition, multiple unauthorized charges appeared on his Walmart account. Indeed, Plaintiff Tetreault was recently informed that his confidential information is on the dark web and has received alerts from fraud monitoring products about potential fraudulent activities.

119. As a result of the Data Breach and as recommended in the Notice, Plaintiff Tetreault made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, checking on credit issues, addressing the Walmart account issue, seeking legal advice/options, maintaining his credit monitoring service from a past data breach, and continually monitoring his credit information and reports Plaintiff Tetreault has spent

significant time, approximately 25-30 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 or recreation. Plaintiff Tetreault suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy, including 1-5 hours each week coping with the impact of cybercriminals accessing and using her PII and PHI.

120. Plaintiff Tetreault does not recall receiving, reviewing or agreeing to Aetna's privacy policies from Aetna or on Aetna's websites. Plaintiff Tetreault believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff Tetreault is unsure, but doubtful, if he would have enrolled with Aetna if he had known Aetna would not adequately protect his PII and PHI. Plaintiff Tetreault is especially concerned about medical fraud and medical disclosures since his medical card number and medical information were involved in this data breach.

121. Thus, as a result of the Data Breach, Plaintiff Tetreault has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Tetreault has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff Gordon Titcomb

122. Plaintiff Gordon Titcomb ("Plaintiff Titcomb") is a citizen and resident of Connecticut.

123. Plaintiff Titcomb has maintained health insurance coverage through Aetna. Aetna required Plaintiff Titcomb to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff

Titcomb's PII and PHI to NationsBenefits after he enrolled with Aetna.

124. Plaintiff Titcomb received a letter dated April 27, 2023, notifying Plaintiff Titcomb that as an insured customer of Aetna his first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, and date of birth were compromised in the Data Breach.

125. Shortly after and as a result of the Data Breach, Plaintiff Titcomb was the victim of fraud and identity theft. Specifically, he experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers, including ones requesting his response and to press a number to respond. In addition, he has received bills for unauthorized charges, such as for computer help and computer updates.

126. As a result of the Data Breach and as recommended in the Notice, Plaintiff Titcomb made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, and continually monitoring his credit information. Plaintiff Titcomb has spent significant time 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 or recreation. Plaintiff Titcomb suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of his privacy, including a fear of financial loss and fear of further privacy loss, over the impact of cybercriminals accessing and using his PII and PHI.

127. Plaintiff Titcomb does not recall receiving, reviewing, or agreeing to Aetna's privacy policies from Aetna or on any of Aetna's websites. Plaintiff Titcomb believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff Titcomb would not have

enrolled with Aetna if she had known Aetna would not adequately protect his PII and PHI.

128. Thus, as a result of the Data Breach, Plaintiff Titcomb has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Titcomb has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff Rodrick Veazey

129. Plaintiff Rodrick Veazey ("Plaintiff Veazey") is a citizen and resident of Florida.

130. Plaintiff Veazey has maintained health insurance coverage through Aetna. Aetna required Plaintiff Veazey to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff Veazey's PII and PHI to NationsBenefits after he enrolled with Aetna.

131. Plaintiff Veazey received a letter dated April 27, 2023, notifying Plaintiff Veazey that as an insured customer of Aetna his first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

132. Shortly after and as a result of the Data Breach, Plaintiff Veazey was the victim of fraud. Specifically, he experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers trying to solicit a response and gain personal information. Indeed, Plaintiff Veazey was recently informed by his bank that his email appeared on the dark web.

133. As a result of the Data Breach and as recommended in the Notice, Plaintiff Veazey made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, closely reviewing financial statements, logging into online accounts

to check activity daily, and continually monitoring his credit information. Plaintiff Veazey has spent significant time 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 or recreation. Plaintiff Veazey suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy, including fear of identity theft, anger at repeated data breaches, and general concern over the impact of cybercriminals accessing and using his PII and PHI.

134. Plaintiff Veazey reviewed and agreed to Aetna's privacy policies he received from Aetna. Plaintiff Veazey believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff Veazey would not have enrolled with Aetna if he had known Aetna would not adequately protect his PII and PHI.

135. Thus, as a result of the Data Breach, Plaintiff Veazey has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Veazey has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff Nicholas Venezia

136. Plaintiff Nicholas Venezia ("Plaintiff N. Venezia") is a citizen and resident of New York.

137. Plaintiff N. Venezia has maintained health insurance coverage through Aetna. Aetna required Plaintiff N. Venezia to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff N. Venezia's PII and PHI to NationsBenefits after he enrolled with Aetna.

138. Plaintiff N. Venezia received a letter dated April 27, 2023, notifying Plaintiff N. Venezia that as an insured customer of Aetna his first name, last name, gender, health plan subscriber identification number, address, phone number, and date of birth were compromised in the Data Breach.

139. Shortly after and as a result of the Data Breach, Plaintiff N. Venezia was the victim of fraud. Specifically, Plaintiff N. Venezia has experienced an increase in spam phone calls.

140. As a result of the Data Breach and as recommended in the Notice, Plaintiff N. Venezia made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, calling Aetna or NationsBenefits, closing the credit card account that was opened in his wife's name, closely reviewing financial statements, logging into online accounts to check activity daily, obtaining credit reports, placing credit holds with credit monitors he already had, and continually monitoring his credit information. Plaintiff N. Venezia has spent significant time, approximately 6 hours in addition to the time spent daily, 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 or recreation. Plaintiff N. Venezia suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced d increased concerns regarding the loss of his privacy, including fear of his information on the dark web, over the impact of cybercriminals accessing and using her PII and PHI.

141. Plaintiff N. Venezia does not recall receiving, reviewing, or agreeing to Aetna's privacy policies from Aetna or on any of Aetna's websites. Plaintiff N. Venezia believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff N. Venezia would not have enrolled with Aetna if he had known Aetna would not adequately protect his PII and PHI.

142. Thus, as a result of the Data Breach, Plaintiff N. Venezia has faced and continues

to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff N. Venezia has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff Valarie Venezia

143. Plaintiff Valarie Venezia ("Plaintiff V. Venezia") is a citizen and resident of New York.

144. Plaintiff V. Venezia has maintained health insurance coverage through Aetna. Aetna required Plaintiff V. Venezia to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff V. Venezia's PII and PHI to NationsBenefits after she enrolled with Aetna.

145. Plaintiff V. Venezia received a letter dated April 27, 2023, notifying Plaintiff V. Venezia that as an insured customer of Aetna her first name, middle initial, last name, gender, health plan subscriber identification number, address, phone number, and date of birth were compromised in the Data Breach.

146. Shortly after and as a result of the Data Breach, Plaintiff V. Venezia was the victim of fraud and identity theft. Specifically, Plaintiff V. Venezia received bills for charges that were not made by her and has experienced health insurance-related fraud since January 2023, as well as a credit card being opened in her name. Additionally, Plaintiff V. Venezia was recently informed that her confidential information is on the dark web.

147. As a result of the Data Breach and as recommended in the Notice, Plaintiff V. Venezia made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, calling Aetna or NationsBenefits to seek information about

the breach, closely reviewing financial statements, logging into online accounts to check activity, obtaining her credit report from the credit reporting agencies, freezing her credit, signing up for credit monitoring – and paying for additional credit monitoring services – and continually monitoring her credit information. Plaintiff V. Venezia has spent significant time responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work or recreation. Plaintiff V. Venezia suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy, including a constant fear of further identity theft, over the impact of cybercriminals accessing and using her PII and PHI.

148. Plaintiff V. Venezia does not recall receiving, reviewing, and agreeing to Aetna's privacy policies from Aetna or on any of Aetna's websites. Plaintiff V. Venezia believed that Aetna would protect her PII and PHI once she provided it to Aetna. Plaintiff V. Venezia would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI.

149. Thus, as a result of the Data Breach, Plaintiff V. Venezia has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff V. Venezia has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff Donna Vogel

150. Plaintiff Donna Vogel ("Plaintiff D. Vogel") is a citizen and resident of Ohio.

151. Plaintiff D. Vogel has maintained health insurance coverage through Aetna. Aetna required Plaintiff D. Vogel to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff D.

Vogel's PII and PHI to NationsBenefits after she enrolled with Aetna.

152. Plaintiff D. Vogel received a letter dated April 27, 2023, notifying Plaintiff D. Vogel that as an insured customer of Aetna her first name, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

153. Shortly after and as a result of the Data Breach, Plaintiff D. Vogel was the victim of fraud. Specifically, she experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers asking her to respond or to press a number "to continue."

154. As a result of the Data Breach and as recommended in the Notice, Plaintiff D. Vogel made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, and continually monitoring her credit information. Plaintiff D. Vogel has spent significant time, approximately 1.5 hours each month, responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work or recreation. Plaintiff D. Vogel suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

155. Plaintiff D. Vogel briefly reviewed the changes made to Aetna's privacy policies, which were sent by Aetna at the beginning of this year. Plaintiff D. Vogel believed that Aetna would protect her PII and PHI once she provided it to Aetna. Plaintiff D. Vogel would not have enrolled with Aetna if she had known Aetna would not adequately protect her PII and PHI.

156. Thus, as a result of the Data Breach, Plaintiff D. Vogel has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff D. Vogel has a continuing interest in ensuring that her PII and PHI, which upon information and belief

remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff John Vogel

157. Plaintiff John Vogel ("Plaintiff J. Vogel") is a citizen and resident of Ohio.

158. Plaintiff J. Vogel has maintained health insurance coverage through Aetna. Aetna required Plaintiff J. Vogel to provide his PII and PHI to Aetna in order to receive health insurance benefits and other services from Aetna. Upon information and belief, Aetna provided Plaintiff J. Vogel's PII and PHI to NationsBenefits after he enrolled with Aetna.

159. Plaintiff J. Vogel received a letter dated April 27, 2023, notifying Plaintiff J. Vogel that as an insured customer of Aetna her first name, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

160. Shortly after and as a result of the Data Breach, Plaintiff J. Vogel was the victim of fraud. Specifically, he experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers, including those asking him to press a number to continue or requesting a response. Plaintiff J. Vogel now usually hangs up before they can say where they are calling from.

161. As a result of the Data Breach and as recommended in the Notice, Plaintiff J. Vogel made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, and continually monitoring his credit information. Plaintiff J. Vogel has spent significant time, approximately 1.5 hours each month, 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. Plaintiff J. Vogel suffered lost time, annoyance,

interference, and inconvenience as a result of the Data Breach. Plaintiff J. Vogel is fearful and concerned someone might end up using his information to make large purchases or create fraudulent accounts as a result of the impact of cybercriminals accessing and using his PII and PHI.

162. Plaintiff J. Vogel briefly reviewed and agreed to Aetna's privacy policies when they mailed him the changes Aetna was making to their policies at the beginning of this year. Plaintiff J. Vogel believed that Aetna would protect his PII and PHI once he provided it to Aetna. Plaintiff J. Vogel would not have enrolled with Aetna if he had known Aetna would not adequately protect his PII and PHI.

163. Thus, as a result of the Data Breach, Plaintiff J. Vogel has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff J. Vogel has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in Aetna's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

164. Plaintiffs Rougeau, Banks, Brewer, Carter, Eddie, Keep, Luciano, Mueller, Peffley-Wilson, Platt, Ronne, Tetreault, Titcomb, Veazey, N. Venezia, V. Venezia, D. Vogel, and J. Vogel are collectively referred to herein as the "Aetna Plaintiffs."

165. Aetna Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI, including, but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

166. Each Aetna Plaintiff suffered a concrete and particularized injury as a result of Aetna's failure to protect their PII and PHI and the subsequent disclosure of their PII and PHI to unauthorized parties without their consent.

167. Had Aetna disclosed that it disregarded its duty to safeguard and protect Aetna Plaintiffs' PII and PHI from unauthorized access, Aetna Plaintiffs would have taken that into account in making their healthcare decisions. In particular, had Aetna Plaintiffs known about Aetna's failure to ensure their vendors and business associates reasonably or adequately secured, safeguarded, and otherwise protected Aetna Plaintiffs' PII and PHI, they would not have provided their PII and PHI to Aetna and would have engaged a competing provider of health insurance benefits.

Plaintiff Ariana Skurauskis

168. Plaintiff Ariana Skurauskis is a resident and citizen of California.

169. Plaintiff Skurauskis has a health plan membership with SCFHP through which she receives health benefits.

170. Plaintiff Skurauskis received a letter from SCFHP dated April 21, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of SCFHP. According to the letter, the compromised files contained Plaintiff Skurauskis' name, contact information, date of birth, Santa Clara Family Health Plan ID number, and Medi-Cal Index Number. Plaintiff Skurauskis has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

171. Plaintiff Skurauskis was the victim of identity theft following Data Breach. After the Data Breach, a large unauthorized charge appeared on her PayPal account. Additionally, in February 2023, an unknown person accessed her Forever 21 account and attempted to purchase

items worth $328.88. Plaintiff Skurauskis has also experienced an increased number of phishing calls and spam text messages since the Data Breach. After the Data Breach, Plaintiff Skurauskis placed a freeze on her credit. Plaintiff Skurauskis is fearful that she will continue to experience identity theft in the future, causing her to lose money, take on increased debt, and negatively affecting her credit score. Plaintiff Skurauskis has experienced increased anxiety as a result of the Data Breach and is anxious and fearful that she will be the victim of identity theft or other fraud in the future because her information was exposed in the Data Breach.

172. Plaintiff Skurauskis reviewed and agreed to SCFHP's privacy policies. Plaintiff Skurauskis believed that SCFHP would protect her PII and PHI once she provided it to SCFHP. Plaintiff Skurauskis would not have enrolled with SCFHP if she had known SCFHP would not adequately protect her PII and PHI.

173. Thus, as a result of the Data Breach, Plaintiff Skurauskis has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Skurauskis has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in SCFHP's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff Renee Rogers

174. Plaintiff Renee Rogers is a resident and citizen of California.

175. Plaintiff Renee Rogers has a health plan membership with SCFHP through which she receives health benefits.

176. Plaintiff Renee Rogers received a letter from SCFHP dated April 21, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of SCFHP. According to the letter, the compromised files contained Plaintiff Renee Rogers'

name, contact information, date of birth, Santa Clara Family Health Plan ID number, and Medi-Cal Index Number. Plaintiff Renee Rogers has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

177. Plaintiff Renee Rogers was the victim of misuse of her Personal Information following the Data Breach. Since the Data Breach, she has experienced an increased number of phishing calls and spam text messages. Plaintiff Renee Rogers is fearful that she will continue to experience misuse of her Personal Information in the future. Plaintiff Renee Rogers has experienced increased concern as a result of the Data Breach and is fearful that she will be the victim of identity theft or other fraud in the future because her information was exposed in the Data Breach.

178. Plaintiff Renee Rogers reviewed and agreed to SCFHP's privacy policies. Plaintiff Renee Rogers believed that SCFHP would protect her PII and PHI once she provided it to SCFHP. Plaintiff Renee Rogers would not have enrolled with SCFHP if she had known SCFHP would not adequately protect her PII and PHI.

179. Thus, as a result of the Data Breach, Plaintiff Renee Rogers has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Renee Rogers has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in SCFHP's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

Plaintiff Noah Rogers

180. Plaintiff Noah Rogers is a resident and citizen of California.

181. Plaintiff Noah Rogers has a health plan membership with Santa Clara Family Health Plan through which he receives health benefits.

182. Plaintiff Noah Rogers received a letter from SCFHP dated April 21, 2023, concerning the Data Breach. The letter stated that unauthorized actors accessed or acquired the data of SCFHP. According to the letter, the compromised files contained Plaintiff Noah Rogers' name, contact information, date of birth, Santa Clara Family Health Plan ID number, and Medi-Cal Index Number. Plaintiff Noah Rogers has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

183. Plaintiff Noah Rogers was the victim of misuse of his Personal Information following the Data Breach. Since the Data Breach, he has experienced an increased number of phishing calls and spam text messages. Plaintiff Noah Rogers is fearful that he will continue to experience misuse of his Personal Information in the future. Plaintiff Noah Rogers has experienced increased concern as a result of the Data Breach and is fearful that he will be the victim of identity theft or other fraud in the future because his information was exposed in the Data Breach.

184. Plaintiff Noah Rogers reviewed and agreed to SCFHP's privacy policies. Plaintiff Noah Rogers believed that SCFHP would protect his PII and PHI once he provided it to SCFHP. Plaintiff Noah Rogers would not have enrolled with SCFHP if he had known SCFHP would not adequately protect his PII and PHI.

185. Thus, as a result of the Data Breach, Plaintiff Noah Rogers has faced and continues to face a present and continuing risk of fraud and identity theft for his lifetime. Plaintiff Noah Rogers has a continuing interest in ensuring that his PII and PHI, which upon information and belief remains backed up in SCFHP's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

186. Plaintiffs Skurauskis, Renee Roger, and Noah Rogers are collectively referred to herein as the "SCFHP Plaintiffs."

Plaintiff Arnisha Shepherd

187. Plaintiff Arnisha Shepherd ("Plaintiff Shepherd") is a citizen and resident of Indiana.

188. Plaintiff Shepherd has maintained health insurance coverage through Anthem. Anthem required Plaintiff Shepherd to provide her PII and PHI to Aetna in order to receive health insurance benefits and other services from Anthem. Upon information and belief, Anthem provided Plaintiff Shepherd's PII and PHI to NationsBenefits after she enrolled with Anthem.

189. Plaintiff Shepherd received a letter dated April 27, 2023, notifying Plaintiff Shepherd that as an insured customer of Anthem her first name, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and medical information were compromised in the Data Breach.

190. Shortly after and as a result of the Data Breach, Plaintiff Shepherd was the victim of fraud and identity theft. Specifically, she experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers, sometimes several in a single day, including those asking if she wants to activate her healthy food card – which she already has, and is active, through NationsBenefits, and suspicious charges to some of her accounts. In addition, she has suffered identity theft having had loans taken out in her name and a cell phone contract with AT&T opened and charged in her name for which AT&T is now pursuing compensation from Plaintiff for the contract which was fraudulently opened.

191. Following the Data Breach, Plaintiff Shepherd has received notice that her Personal Information has been found on the dark web. Plaintiff Shepherd received no such notice prior to this Data Breach.

192. As a result of the Data Breach and as recommended in the Notice, Plaintiff

Shepherd made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, hiring an attorney to fight the action taken by AT&T, monitoring her credit reports through CreditKarma, and discussing what to do next with an attorney. Plaintiff Shepherd has spent significant time, approximately 50-60 hours to date, responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work or recreation. Plaintiff Shepherd suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy over the impact of cybercriminals accessing and using her PII and PHI.

193. Plaintiff Shepherd does not recall receiving, reviewing, or agreeing to Anthem's privacy policies from Anthem or on Anthem's website. Plaintiff Shepherd reasonably believed that Anthem would protect her PII and PHI once she provided it to Anthem. Plaintiff Shepherd would not have enrolled with Anthem if she had known Anthem would not adequately protect her PII and PHI.

194. Thus, as a result of the Data Breach, Plaintiff Shepherd has faced and continues to face a present and continuing risk of fraud and identity theft for the remainder of her lifetime.[16] Plaintiff Shepherd has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Anthem's and NationsBenefits' possession, is protected and safeguarded from future data breaches.

[16] The value of information grows as it is a cumulative effect. Any subsequent data breaches would only add to the already existing compromised information and allow thieves and criminals to build on what is leaked by Defendant.

Plaintiff Shontay Marshall

195. Plaintiff Shontay Marshall ("Plaintiff Marshall") is a citizen and resident of Kentucky.

196. Plaintiff Marshall has maintained health insurance coverage through Elevance. Elevance required Plaintiff Marshall to provide her PII and PHI to Elevance in order to receive health insurance benefits and other services from Elevance. Upon information and belief, Elevance provided Plaintiff Marshall's PII and PHI to NationsBenefits after she enrolled with Elevance.

197. Plaintiff Marshall received a letter dated April 27, 2023, notifying Plaintiff Marshall that as an insured customer of Elevance her first name, last name, gender, health plan subscriber identification number, address, phone number, date of birth, and Medicare number were compromised in the Data Breach.

198. Shortly after and as a result of the Data Breach, Plaintiff Marshall was the victim of fraud and identity theft. Specifically, she experienced a large increase in spam and suspicious phone calls, texts, and emails from strangers, sometimes several in a single day, including those asking if she wants to activate her healthy food card – which she already has, and is active, through NationsBenefits, and suspicious charges to some of her accounts.

199. As a result of the Data Breach and as recommended in the Notice, Plaintiff Marshall made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach, closely reviewing financial statements, logging into online accounts to check activity, monitoring her credit reports, and discussing what to do next with an attorney. Plaintiff Marshall has spent significant time, approximately 10-20 hours to date, responding to the Data Breach and will continue to spend valuable time she otherwise would have spent on other activities, including, but not limited to, work or recreation. Plaintiff Marshall suffered lost time,

annoyance, interference, and inconvenience as a result of the Data Breach and has experienced increased concerns regarding the loss of her privacy over the impact of cybercriminals accessing and using her PII and PHI.

200. Plaintiff Marshall does not recall receiving, reviewing, or agreeing to Elevance's privacy policies from Elevance or on Elevance's website. Plaintiff Marshall believed that Elevance would protect her PII and PHI once she provided it to Elevance. Plaintiff Marshall would not have enrolled with Elevance if she had known Elevance would not adequately protect her PII and PHI.

201. Thus, as a result of the Data Breach, Plaintiff Marshall has faced and continues to face a present and continuing risk of fraud and identity theft for her lifetime. Plaintiff Marshall has a continuing interest in ensuring that her PII and PHI, which upon information and belief remains backed up in Elevance's and NationsBenefits' possession, is protected and safeguarded from future data breaches

B. Defendants

202. Defendant Aetna Inc. is Pennsylvania corporation with its principal place of business located at 151 Farmington Ave, Hartford, Connecticut 06156.

203. Defendant Aetna Life Insurance Company is a Connecticut corporation with its principal place of business located at 151 Farmington Ave., Hartford, Connecticut 06156 and is a wholly owned subsidiary of Aetna Inc. Aetna Life Insurance Company is authorized to conduct business and does conduct business in the State of Florida.

204. Defendant SCFHP is a community-based health plan located in San Jose, California serving hundreds of thousands of people through its various product offerings, including Medi-Cal, Cal MediConnect, and SCFHP DualConnect healthcare plans.

205. Defendant Anthem is a national health insurance company pursuant to state and

federal law, providing health insurance and medical services to the general public, operating at 120 Monument Circle, Indianapolis, IN 46204. Anthem is authorized to conduct business and does conduct business in the State of Florida.

206. Defendant Elevance Health, Inc. is a nationwide health insurance provider with its headquarters and principal place of business located in Indianapolis, Indiana. Elevance Health, Inc. is authorized to conduct business and does conduct business in the State of Florida.

IV. FACTUAL ALLEGATIONS

A. Defendant Aetna

207. Aetna is a leading provider of health insurance services in the United States. Aetna offers a range of healthcare products and services to employers, individuals, college students, and part-time and hourly workers nationwide. Aetna is a "Covered Entity" under HIPAA.

208. Aetna's health insurance offerings include medical, pharmacy, dental, behavioral health, group life, and disability plans, and several Medicare offerings, including Medicare Advantage.

209. Aetna's Medicare Advantage plans are an alternative to Medicare Parts A and B, and often incorporate prescription drug coverage (Part D), as well as additional benefits not covered by Medicare such as vision, hearing, and dental care.

210. Aetna also offers Medicare Supplement Insurance, or "Medigap" plans, which help cover some of the healthcare costs that Medicare doesn't pay, standalone prescription drug (Part D) plans, and a combination plan called the Aetna Dual Eligible Special Needs Plan ("D-SNP") for those eligible for both Medicare and Medicaid.

211. As part of its Medicare plan offerings, Aetna partners with NationsBenefits to provide certain benefits to its members such as Aetna Plaintiffs and Class Members. NationsBenefits is Aetna's HIPAA Business Associate.

212. Individuals such as Aetna Plaintiffs and Class Members who enroll with Aetna are required, by Aetna, to provide sensitive PII and PHI.

213. Aetna, through privacy policies, codes of conduct, company security practices, and other conduct, implicitly and explicitly promised to safeguard Aetna Plaintiffs' and Class Members' PII and PHI.

214. Aetna's Medicare Notice of Privacy Practices ("Medicare Privacy Policy"), states it collects PII and PHI from Aetna Plaintiffs and Class Members relating to an individual's "health, medical conditions, prescriptions, and payment for health care products or services," such as demographic data, health details, test results, insurance information, and other information used to identify an individual or that is linked to an individual's health care or health care coverage.[17]

215. Aetna and its affiliates have a non-delegable duty under federal law to ensure that all member information it collects and stores is secure, and that any vendors or business associates with whom it shares information also maintain adequate and commercially reasonable data security practices to ensure the protection of members' PII and PHI.

216. Indeed, Aetna's entire business depends on members entrusting it with their PII and PHI. Without insureds' PII and PHI, Aetna would not be able to provide health insurance benefits and other services and certainly would not be able to bill insureds and collect payment for health insurance benefits and other services rendered. More specifically, to provide health insurance benefits, Aetna knows that its insureds must trust that Aetna is keeping their PII and PHI private

[17] *Medicare Notice of Privacy Practices*, Aetna, https://www.aetnamedicare.com/content/dam/aetna/pdfs/wwwaetnamedicarecomSSL/individual/2022/member/Notice_of_Privacy_Policies.pdf.

and secure. If Aetna's insureds lack trust in Aetna or knew Aetna would insecurely store, safeguard, or transmit their PII and PHI, then they will not disclose that information to it and would choose a competitor for health insurance benefits and other services.

Defendant SCFHP

217. Founded in 1997, SCFHP is a community-based health plan located in San Jose, California serving hundreds of thousands of individuals through its various product offerings, including Medi-Cal, Cal MediConnect, and DualConnect healthcare plans. SCFHP is a "Covered Entity" under HIPAA

218. SCFHP employs more than 241 people and generates approximately $75 million in annual revenue.

219. As a condition of receiving healthcare plans and services, Defendant requires that its members turn over highly sensitive personal and health information. In the ordinary course of receiving service from Defendant, SFCHP Plaintiffs and Class Members were required to provide their Personal Information.

220. Upon information and belief, SCFHP partners with NationsBenefits to provide certain benefits to its members such as SCFHP Plaintiffs and Class Members. NationsBenefits is SFCHP's HIPAA Business Associate.

221. In its Notice of Privacy Practices (also referred to herein as the "Privacy Policy"), SCFHP makes clear that it is "required by state and federal law to protect your health information."[18] SCFHP also describes in its Privacy Policy the limited specific instances when it

[18] *See* https://www.scfhp.com/privacy-policy/#:~:text=Your%20Information%20is%20Personal%20and,pay%20for%20your%20health%20care.

shares its members' health information and says that in order for such sharing to occur, "we must get your written permission."[19]

222. SCFHP uses this information, *inter alia*, "[f]or treatment," "[f]or payment," "[f]or health care operations," and "[f]or business associates . . . that assist[] us in operating our health system."[20]

223. SCFHP Plaintiffs and Class Members relied on SCFHP's promise to keep their Personal Information confidential and securely maintained, and to only make authorized disclosures of this information. SCFHP failed to do so.

224. SCFHP Plaintiffs and Class Members also relied on SCFHP to ensure that it held vendors with whom it shared sensitive Personal Information to the same high standards of data protection. SCFHP failed to do so.

225. SCFHP and its affiliates have a non-delegable duty under federal law to ensure that all member information it collects and stores is secure, and that any vendors or business associates with whom it shares information also maintain adequate and commercially reasonable data security practices to ensure the protection of members' PII and PHI.

226. Indeed, SCFHP's entire business depends on members entrusting it with their PII and PHI. Without insureds' PII and PHI, SCFHP would not be able to provide health insurance benefits and other services and certainly would not be able to bill insureds and collect payment for health insurance benefits and other services rendered. More specifically, to provide health insurance benefits, SCFHP knows that its insureds must trust that Anthem is keeping their PII and PHI private and secure. If SCFHP's insureds lack trust in SCFHP or knew SCFHP would

[19] *Id.*
[20] *Id.*

insecurely store, safeguard, or transmit their PII and PHI, then they will not disclose that information to it and would choose a competitor for health insurance benefits and other services.

Defendant Anthem

227. Defendant Anthem is a national health insurance company pursuant to state and federal law, providing health insurance and medical services to the general public. Anthem is a "Covered Entity" under HIPAA.

228. As a part of its business operations, Anthem collect and maintain PHI and PII of its customers.

243. Upon information and belief, Anthem partners with NationsBenefits to provide certain benefits to its members such as Plaintiff Shepherd and Class Members. NationsBenefits is Anthem's HIPAA Business Associate.

244. Individuals such as Plaintiff Shepherd and Class Members who enroll with Anthem are required, by Anthem, to provide sensitive PII and PHI.

245. Anthem, through privacy policies, codes of conduct, company security practices, and other conduct, implicitly and explicitly promised to safeguard Plaintiff Shepherd and Class Members' PII and PHI.

246. Defendant Anthem posts its privacy practices online, at https://www.anthem.com/privacy/

247. Anthem and its affiliates have a non-delegable duty under federal law to ensure that all member information it collects and stores is secure, and that any vendors or business associates with whom it shares information also maintain adequate and commercially reasonable data security practices to ensure the protection of members' PII and PHI.

248. Indeed, Anthem's entire business depends on members entrusting it with their PII and PHI. Without insureds' PII and PHI, Anthem would not be able to provide health insurance benefits and other services and certainly would not be able to bill insureds and collect payment for health insurance benefits and other services rendered. More specifically, to provide health insurance benefits, Anthem knows that its insureds must trust that Anthem is keeping their PII and PHI private and secure. If Anthem's insureds lack trust in Anthem or knew Anthem would insecurely store, safeguard, or transmit their PII and PHI, then they will not disclose that information to it and would choose a competitor for health insurance benefits and other services.

Defendant Elevance

249. Founded in 1946 as Anthem, Inc., Elevance is a nationwide health insurance provider.[21]

250. When Elevance collects sensitive information, it promises to use reasonable measures to safeguard the PII and PHI from theft and misuse.

251. Elevance acquired, collected, and stored, and represented that it maintained reasonable security over Plaintiff Marshall's and Class Members' PII and PHI.

252. By obtaining, collecting, receiving, and/or storing Plaintiff Marshall's and Class Members' PII and PHI, Elevance assumed legal and equitable duties and knew, or should have known, that it was thereafter responsible for protecting Plaintiff Marshall's and Class Members' PII and PHI from unauthorized disclosure.

253. On Elevance's Privacy Policy, published on its website ("Privacy Policy"), Elevance represents and promises, "Your privacy is very important to us and we will make every reasonable effort to safeguard any information we collect."[22]

[21] https://www.elevancehealth.com/.
[22] https://www.elevancehealth.com/privacy-policy.

254. Elevance's Privacy Policy applies to both its employees and non-employee members/customers.

255. Elevance and its affiliates have a non-delegable duty under federal law to ensure that all member information it collects and stores is secure, and that any vendors or business associates with whom it shares information also maintain adequate and commercially reasonable data security practices to ensure the protection of members' PII and PHI.

256. Indeed, Elevance's entire business depends on members entrusting it with their PII and PHI. Without insureds' PII and PHI, Elevance would not be able to provide health insurance benefits and other services and certainly would not be able to bill insureds and collect payment for health insurance benefits and other services rendered. More specifically, to provide health insurance benefits, Elevance knows that its insureds must trust that Elevance is keeping their PII and PHI private and secure. If Elevance's insureds lack trust in Elevance or knew Elevance would insecurely store, safeguard, or transmit their PII and PHI, then they will not disclose that information to it and would choose a competitor for health insurance benefits and other services.

Defendants are Covered Entities Pursuant to State and Federal Law

257. Defendants, and each of them, are covered entities under HIPAA. *See* 45 C.F.R. § 160.102. Defendants must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

258. The duties of privacy imposed by state and federal law as well as each Defendants' own policies and procedures, is a non-delegable duty which independently attaches to each covered entity.

259. Defendants are covered entities pursuant to the Health Information Technology Act ("HITECH")[23]. *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

260. The HIPAA and HITECH rules work in conjunction with the already established laws of privacy in each state. HIPAA and HITECH do not recognize an individual right of claim for violation but provide the guidelines for the standard of procedure dictating how patient medical information should be kept private.

261. HIPAA's Privacy Rule, otherwise known as "Standards for Privacy of Individually Identifiable Health Information," establishes national standards for the protection of health information.

262. HIPAA and HITECH require covered entities to create and implement policies and procedures, consistent with HIPAA and HITECH, within the covered entities own company.[24]

263. HIPAA's Security Rule, otherwise known as "Security Standards for the Protection of Electronic Protected Health Information," establishes national security standards for the protection of health information that is held or transferred in electronic form. See 42 C.F.R. §§ 164.302-164.318.

264. HIPAA limits the permissible uses of "protected health information" and prohibits the unauthorized disclosure of "protected health information." 45 C.F.R. § 164.502. HIPAA requires that covered entities implement appropriate administrative, technical, and physical safeguards for this information and requires that covered entities reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the

[23] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

[24] In other words, the privacy policies and procedures applicable to the protection of PHI and PII must match the rules and regulations of HIPAA and HITECH.

standards, implementation specifications or other requirements of this subpart. *See* 45 C.F.R. § 164.530(c).

265. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

266. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

267. Under HIPAA:

> Protected health information means individually identifiable health information:
>
> (1) Except as provided in paragraph (2) of this definition, that is:
> (i) Transmitted by electronic media;
> (ii) Maintained in electronic media; or
> (iii) Transmitted or maintained in any other form or medium.[25]

268. HIPAA and HITECH obligated Defendants to implement technical policies and procedures for electronic information systems that maintain electronic protected health information so that such systems were accessible only to those persons or software programs that had been granted access rights and who have a working need to access and view the information. *See* 45 C.F.R. § 164.312(a)(1); *see also* 42 U.S.C. § 17902.

269. HIPAA and HITECH also obligated Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not

[25] 45 C.F.R. § 160.103

permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

270. HIPAA further obligated Defendants to ensure that its workforce complied with HIPAA security standard rules (*see* 45 C.F.R. § 164.306(a)(4)) to effectively train its workforces on the policies and procedures with respect to protected health information, as necessary and appropriate for those individuals to carry out their functions and maintain the security of protected health information. *See* 45 C.F.R. § 164.530(b)(1).

271. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." *See* US Department of Health & Human Services, Security Rule Guidance Material.[26] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represents the industry standard for good business practices with respect to standards for securing e-PHI." *See* US Department of Health & Human Services, Guidance on Risk Analysis.[27]

272. Should a health care provider experience an unauthorized disclosure, it is required to conduct a Four Factor Risk Assessment (HIPAA Omnibus Rule). This standard requires, "A covered entity or business associate must now undertake a four-factor risk assessment to determine

[26] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
[27] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

whether or not PHI has been compromised and overcome the presumption that the breach must be reported. The four-factor risk assessment focuses on:

> (1) the nature and extent of the PHI involved in the incident (e.g., whether the incident involved sensitive information like social security numbers or infectious disease test results);
> (2) the recipient of the PHI;
> (3) whether the PHI was actually acquired or viewed; and
> (4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (e.g., whether it was immediately sequestered and destroyed)."[28]

273. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

274. The HIPAA Contingency Operations Rule, 45 C.F.R. §164.301(a), requires a healthcare provider to have security measures in place and train its employees and staff so that all its staff and employees know their rolls in facility security.

275. Defendants, however, failed to adhere to its legal duties to protect Plaintiffs' and Class Members' PII and PHI.

276. The above-listed duties apply equally to HIPAA covered entities, like Defendants, and their HIPAA business associates, like NationsBenefits, and Defendants had non-delegable duties to monitor, oversee, and ensure compliance by NationsBenefits. They failed to do so.

B. Defendants Collect Patient and Customer PII and PHI for Their Own Commercial, Financial Benefit.

277. Defendants outsource several benefits and services its health plan holders are entitled to third-party vendor providers rather than provide those benefits to Defendants' patients and customers. One such third-party vendor provider Defendants sourced the provision of benefits

[28] 78 Fed. Reg. 5641-46, *See also*, 45 C.F.R. §164.304

to is NationsBenefits. However, prior to sharing PII and PHI with any vendor, Defendants must first enter into a Business Associate Agreement with such vendor under which the vendor warrants to also comply with HIPAA's data security requirements.

278. Each Defendant derives financial benefit from its partnership with NationsBenefits. According to NationsBenefits, for health plans, "partnering with a leading supplemental benefits, such as NationsBenefits, is a key component for successfully… [r]educing [c]osts" as well as "[e]nabling [g]rowth and [r]etention."[29]

279. NationsBenefits describes itself as "a leading provider of supplemental benefits, flex cards, and member engagement solutions that partners with managed care organizations to provide innovative healthcare solutions designed to drive growth, improve outcomes, reduce costs, and delight members."[30]

280. NationsBenefits provides these services through a "comprehensive suite of innovative supplemental benefits, payments platform, and member engagement solutions [which] help health plans deliver high quality benefits to their members that help address social determinants of health and improve member health outcomes and satisfaction."[31]

281. In doing so, Defendants provided the PII and PHI of millions of patients and customers to NationsBenefits without adequately reviewing and evaluating NationsBenefits' information technology security and systems, as they were legally required to do as HIPAA covered entities.

282. Worse, it appears that Defendants provided the information of millions of patients and customers to NationsBenefits *before* Defendants' patients and customers attempted to use the

[29] https://www.nationsbenefits.com/health-plans .
[30] https://www.nationsbenefits.com/about-us .
[31] *Id.*

programs offered by NationsBenefits, resulting in Defendants sharing the PII and PHI of millions of patients and customers who never interacted with NationsBenefits at all and when Defendants had no legitimate business need to do so.

283. As such, Defendants affirmatively disclosed Plaintiffs' and Class members' PII and PHI to NationsBenefits without consent, without any legitimate business need to do so, and when NationsBenefits was not authorized to receive the information.

284. Even assuming Defendants had a legitimate business reason to disclose PII and PHI to NationsBenefits before any member desired to use its services, Defendants had duties to ensure that each of its third-party vendors and HIPAA business associates, including NationsBenefits, adopted reasonable measures to protect the PII and PHI of Plaintiffs and Class Members from involuntary disclosure to third parties.

285. Therefore, Plaintiffs and Class Members reasonably relied on Defendants to adequately review and evaluate the information technology security systems of vendors, such as NationsBenefits, and to ensure that their PII and PHI provided to the vendors chosen by Defendants would remain confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

C. The Data Breach Is Announced

286. To provide the services outlined above and others, NationsBenefits used the GoAnywhere MFT software provided by third-party vendor Fortra to exchange files with Defendants containing the PII and PHI of Plaintiffs and Class Members.

287. Upon information and belief, Defendants have sufficient control over Fortra's file transfer platform GoAnywhere to properly secure and encrypt Plaintiffs' and Class Members' data that it exchanged with NationsBenefits over the GoAnywhere platform.

288. Unfortunately for Plaintiffs and Class Members, the Data Breach occurred, when from January 28, 2023, through February 7, 2023, an unauthorized third-party hacker group exploited a vulnerability in the Fortra GoAnywhere MFT software and began accessing and exfiltrating Plaintiffs' and Class Members' PII and PHI, which previously had been exchanged between Defendants and NationsBenefits via the Fortra GoAnywhere MFT software.

289. NationsBenefits purportedly became aware of the Data Breach on February 7, 2023. NationsBenefits then notified Defendants of the Data Breach on or around February 9, 2023. Yet Plaintiffs and Class Members were not notified of the Data Breach until sometime after April 27, 2023, when *NationsBenefits* (not Defendants) mailed out notification letters to individuals whose information had been compromised. Most individuals did not receive the letters until early May 2023. This nearly three-month delay deprived Plaintiffs and Class Members of the ability to take steps to mitigate the damages caused by the Data Breach.

290. Below are relevant excerpts from the letters sent to Plaintiffs and the Class Members whose information was compromised in the Data Breach ("Notice of Data Breach" or "Notice"):

> NationsBenefits Holding, LLC, and its affiliates and subsidiaries (collectively, "NationsBenefits" or "we"), provides benefits administration services to your health insurer, [client_name]. We place a high value on maintaining the privacy and security of the information we maintain for our health plan customers. Regrettably, this letter is to inform you that a vendor we used to exchange files with Aetna[32] was recently the victim of a cybersecurity attack, which impacted some of your personal information. We notified [Defendant] of this incident [on February 9, 2023]. This letter explains the incident, the measures we have taken in response and the steps you can take.
>
> What Happened? NationsBenefits used software provided by a third-party vendor, Fortra, LLC ("Fortra"), to securely exchange files with your health plan. On or around January 30, 2023, Fortra experienced a data security incident in which a malicious actor(s) accessed or acquired the data of multiple organizations,

[32] https://www.hipaajournal.com/nationsbenefits-holdings-confirms-3-million-record-data-breach; *see also* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf .

> including NationsBenefits. When we learned of this incident on February 7, 2023, we immediately took steps to secure our systems and launched an investigation, which was conducted by an experienced outside law firm and a leading cybersecurity firm. As part of our investigation, NationsBenefits analyzed the impacted data to determine whether any individual's personal information was subject to unauthorized access or acquisition. On February 23, 2023, NationsBenefits confirmed that, unfortunately, some of your personal information was affected by the incident.[33]

291. Upon information and belief, the Notice of Data Breach was drafted and publicized under the direction and with the approval of each Defendant.

292. NationsBenefits' filing with the U.S. Department of Health and Human Services ("HHS") and public reporting has revealed that the PII and PHI of millions of patients and customers of Defendants was compromised in the Data Breach and that "[t]he compromised information included: first and last name, address, phone number, date of birth, gender, health plan subscriber ID number, Social Security number, and/or Medicare number."[34]

293. NationsBenefits' filing with the Office of the Maine Attorney General has further confirmed that the PII and PHI compromised in the Data Breach includes names and other personal identifiers "in combination with" Social Security Number(s).[35]

294. The Notice recommended Plaintiffs and Class Members to "remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity" and to follow the below steps to further protect themselves:

a. order your free credit report;

b. if you believe you are the victim of identity theft or have reason to believe your personal information has been misused, contact the FTC and/or your state's

[33] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-187.pdf .
[34] https://www.hipaajournal.com/nationsbenefits-holdings-confirms-3-million-record-data-breach/.
[35] https://apps.web.maine.gov/online/aeviewer/ME/40/764dec53-ed17-4732-9d8b-111239af9176.shtml.

attorney general office about for information on how to prevent or avoid identity theft;

c. place a security freeze; and

d. place a fraud alert.[36]

295. Defendants thus largely placed the burden on Plaintiffs and Class Members to take measures to protect themselves.

296. Defendants, through NationsBenefits, also offered credit monitoring services to some Class Members for a period of 24 months. Such measures, however, are insufficient to protect Plaintiffs and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiffs and Class Members seek a sum of money sufficient to provide Plaintiffs and Class Members identity theft protection services for their respective lifetimes.

297. Defendants had a non-delegable duty to ensure that their systems, policies, and those of their vendors and HIPAA business associates, including NationsBenefits, were sufficient to adequately secure Defendants' insureds' PII and PHI. By failing to adequately monitor and audit the data security systems of NationsBenefits, Defendants put members' PII and PHI at severe risk.

298. As evidenced by the Notice of Data Breach, Defendants failed to:

a. properly secure and encrypt Plaintiffs' and Class Members' data that Defendants exchanged with NationsBenefits over the GoAnywhere platform;[37]

b. ensure that its HIPAA business associates ensured the proper encryption of Plaintiffs' and Class Members' PII and PHI;[38]

[36] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-187.pdf.
[37] *Id.* ("NationsBenefits confirmed that, unfortunately, some of your personal information was affected by the incident.").
[38] *Id.*

c. properly select and supervise its HIPAA business associates and ensure their compliance with HIPAA;[39]

d. ensure that its HIPAA business associates properly monitored and logged the ingress and egress of network traffic involving Plaintiffs' and Class Members' sensitive data;[40]

e. ensure that its HIPAA business associates s implemented sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.[41]

D. Defendants Failed to Provide Proper Notice of the Data Breach

299. As detailed above, Defendants have never directly notified their patients and customers that their information has been compromised in the Data Breach. Moreover, while NationsBenefits has stated it learned of the Data Breach on January 30, 2023, NationsBenefits failed to even begin notifying Plaintiffs and Class Members until April 27, 2023, via U.S. Mail.

300. Defendants appear to have disavowed any duty to notify its members of the Data Breach, and instead deferred to NationsBenefits' decision to choose to notify individuals only via U.S. mail, even though both Defendants and NationsBenefits possesses telephone and email contact information for each customer, which is likely more effective at reaching those individuals than U.S. mail.

301. Additionally, the three-month delay—a facially unreasonable amount of time under any measure—prevented Plaintiffs and Class Members from taking steps to mitigate the damage caused by the Data Breach.

---

[39] *Id.*

[40] *Id.* ("On or around January 30, 2023, Fortra experienced a data security incident in which a malicious actor(s) accessed or acquired the data of multiple organizations, including NationsBenefits," but NationsBenefits did not "learn[] of this incident [until] February 7, 2023".).

[41] *Id.*

302. Instead, and to protect its own financial interests, Defendants concealed the Data Breach for almost three months, allowing the unauthorized third-party to potentially exploit Plaintiffs' and Class Members' PII and PHI without any mitigation steps being taken. Aetna did this despite knowing that the information was in possession of bad actors looking to exploit the PII and PHI for profit, a fact that Defendants knew shortly after discovery of the Data Breach.

303. Plaintiffs and Class Members were thus deprived of the opportunity to take any steps to prevent damage by Defendants' concealment of the Data Breach and failure to provide timely and adequate notice of the Data Breach to Plaintiffs and Class Members.

E. Defendants Failed to Exercise Due Care in Compliance with FTC Guidance and Industry Standards.

304. Federal and state governments have established security standards and issued recommendations to reduce the number and size of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses, highlighting the importance of reasonable data and cyber security practices. According to the FTC, the need for data and cyber security should be factored into all business decision-making.[42]

305. Defendants are prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." 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 the FTC Act.

[42] *Start with Security: A Guide for Business* at 2, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

306. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which established guidelines for fundamental data and cyber security principles and practices for business.[43] The guidelines note businesses should protect the personal customer and consumer 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 security problems.[44] 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.[45]

307. The FTC recommends that companies 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 (most pertinent here) verify, monitory, and audit that third-party service providers have implemented reasonable security measures.

308. 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 FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[43] *Protecting Private Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business [https://perma.cc/9945-U4HV].
[44] *Id.*
[45] *Id.*

309. These FTC enforcement actions include actions against healthcare providers and partners like each Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

310. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to members' PII and PHI, specifically by failing to verify, monitor, and audit that their HIPAA business associates have implemented reasonable security measures, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

311. Defendants also have obligations created by other federal and state laws and regulations, contracts, industry standards, and common law to maintain reasonable and appropriate physical, administrative, and technical measures to keep Plaintiffs' and Class Members' PII and PHI confidential and to protect it from unauthorized access and disclosure.

312. Given the magnitude of the risk and repercussions of a data breach or attack targeting this type of data, the likelihood of a data breach or attack, and Defendants' explicit awareness of these vulnerabilities, Defendants should have taken every reasonable precaution in developing a robust security program and vendor risk-management program and protecting Plaintiffs' and the Class Members' PII and PHI.

313. Yet, despite its duties, representations, and promises, Defendants failed to adequately secure and protect their customers' data, allowing the Plaintiffs' and Class Members' PII and PHI to be accessed, disclosed, and misused.

314. Defendants also owed a duty to comply with industry standards in safeguarding PII and PHI, which—as discussed herein—they did not do.

315. Cyberattacks have become so notorious that the FBI and Secret Service issued an unprecedented warning in 2019 to potential targets so they were aware of, and prepared for, a potential attack.[46]

316. The U.S. government, various U.S. and international law enforcement agencies, cybersecurity industry groups and laboratories, and numerous industry trade groups have issued warnings and guidance on managing and mitigating phishing and ransomware threats. There are industry best practices for cybersecurity related to phishing and ransomware, some of which are particularly effective.

317. For example, in 2019, both Microsoft and Google publicly reported that using multi-factor authentication ("MFA") blocks more than 99% of automated hacks, including most ransomware attacks that occur because of unauthorized account access. Likewise, the reputable SANS Software Security Institute issued a paper stating "[t]ime to implement multi-factor authentication!"[47] An example of MFA implementation is receiving a text with a code when you input your username and password into a website; even if a cybercriminal knew your username and password, the cybercriminal would not be able to see the code on your phone and would thus be blocked from accessing your online account.

318. In this regard, implementing MFA "can block over 99.9 percent of account compromise attacks."[48]

---

[46] Kochman, *supra* n.171.

[47] Matt Bromiley, *Bye Passwords: New Ways to Authenticate* at 3, SANS Software Security Inst. (July 2019), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ [https://perma.cc/ZSW9-QUEW]. Matt Bromiley, *Bye Passwords: New Ways to Authenticate* at 3, SANS Software Security Inst. (July 2019), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ [https://perma.cc/ZSW9-QUEW].

[48] *What Is Multi-Factor Authentication (MFA)?*, Consensus Techs. (Sept. 16, 2020), https://www.concensus.com/what-is-multi-factor-authentication/#:~:text=The%20proof%20that%20MFA%20works,percent%20of%20account%20compromise%20attacks [https://perma.cc/RKT2-LX5Z].

319. Because of the value of PII and PHI to hackers and identity thieves, companies in the business of obtaining, storing, maintaining, and securing PII and PHI, such as Defendants, have been identified as being particularly vulnerable to cyber-attacks. Cybersecurity firms have promulgated a series of best practices that at minimum should be implemented by sector participants including, but not limited to: 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 protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.[49]

320. Other best practices have been identified that at a minimum should be implemented by health 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.

321. Yet, instead of following these widely adopted industry standards, Defendants failed to adequately secure and protect their customers' data, allowing the Plaintiffs' and Class Members' PII and PHI to be accessed, disclosed, and misused by failing to verify, monitor, and audit that HIPAA business associates have implemented reasonable security measures.

F. Plaintiffs' and the Class Members' PII and PHI Is Highly Valuable.

322. Defendants understand the protected PII and PHI that they acquire, store, and utilize is highly sensitive and of significant value to the owners of the PII and PHI and those who would use it for wrongful purposes.

[49] *See Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, Inc. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security/ [https://perma.cc/NY6X-TFUY].

323. The healthcare industry in particular has experienced a large number of high-profile cyberattacks even in just the short period preceding the filing of this Complaint, and cyberattacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25% increase.[50] Additionally, according to the HIPAA Journal, the largest healthcare data breaches have been reported beginning in April 2021.[51]

324. In the context of data breaches, healthcare is "by far the most affected industry sector."[52] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[53] And according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[54]

325. Despite the prevalence of public announcements of data breaches and data security compromises, Defendants failed to take appropriate steps to protect Plaintiffs' and Class Members' PII and PHI from being compromised.

(i) The Value of PII and PHI

326. Personal Information, such as PII and PHI, is property with inherent and sizeable market value. Its value is axiomatic, considering the market value and profitability of "Big Data" corporations in America. Alphabet Inc., the parent company of Google, aptly illustrated this in its 2020 Annual Report, when it reported a total annual revenue of $182.5 billion and net income of

---

[50] *2020 Healthcare Data Breach Report,* HIPAA JOURNAL (Jan. 19, 2021) https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/.

[51] *April 2021 Healthcare Data Breach Report,* HIPAA JOURNAL (May 18, 2021) https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/.

[52] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches.

[53] *See id.*

[54] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

$40.2 billion.[55] $160.7 billion of this revenue was derived from its Google business, which is driven almost exclusively by leveraging the PII and PHI it collects about the users of its various free products and services. America's largest corporations profit almost exclusively through the use of PII and PHI, illustrating the considerable market value of PII and PHI.

327. Criminal law also recognizes the value of PII and PHI and the serious nature of the theft of such an asset by imposing prison sentences. This strong deterrence is necessary because cybercriminals earn significant revenue through stealing PII and PHI. Once a cybercriminal has unlawfully acquired personal data, the criminal can demand a ransom or blackmail payment for its destruction, use the information to commit fraud or identity theft, or sell the PII and PHI to another cybercriminal on a thriving black market.

328. Furthermore, Personal Information, such as PII and PHI, is a valuable commodity to identity thieves, particularly when such data is aggregated in large numbers. Former United States Attorney General William P. Barr made clear that consumers' sensitive personal information commonly stolen in data breaches "has economic value." The purpose of stealing large caches of personal data is to use it to defraud individuals or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit fraud and identity theft. Indeed, cybercriminals routinely post stolen personal information for sale on anonymous websites, making the information widely available to a criminal underworld.

329. There is an active and robust market for this information. As John Sancenito, president of Information Network Associates, a company which helps companies with recovery after data breaches, explained after a data breach "[m]ost of the time what [data breach hackers]

[55] Alphabet Inc., Annual Report (Form 10-K) at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.

do is they steal the data and then they sell the data on the dark web to the people who actually commit the fraud."

330. Thus, Plaintiffs and Class Members rightfully place a high value not only on their PII and PHI, and on the privacy of that data.

331. Once stolen, PII and PHI can be used in a number of different ways. One of the most common is that it is offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items, such as weapons, drugs, and PII and PHI. Websites appear and disappear quickly, making it a dynamic environment.

332. The forms of PII and PHI involved in this Data Breach are particularly concerning. Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique Medicare ID numbers, health plan ID numbers, and Social Security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies to update the person's accounts with those entities.

333. Another example of criminals using PII and PHI for profit is the development of "Fullz" packages.[56]

[56] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which

334. Cyber-criminals can cross-reference two sources of PII and PHI 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.

335. The development of "Fullz" packages means that stolen PII and PHI from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' 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 and PHI 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 Class Members of, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and other Class Members' stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

(ii) Data breaches put patients and consumers at increased risk of fraud and identity theft.

336. Cyberattacks and data breaches of health services companies are especially problematic because of the potentially permanent disruption they cause to the daily lives of their

are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014) https://krebsonsecurity.com/tag/fullz/.

customers. Stories of identity theft and fraud abound, with hundreds of millions of dollars lost by everyday consumers every year as a result of internet-based identity theft attacks.[57]

337. The U.S. Government Accountability Office ("GAO") released a report in 2007 regarding data breaches, finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[58]

338. The FTC recommends that identity theft victims take several steps to protect their personal health and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), 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.[59]

339. Cybercriminals use stolen PII and PHI, such as Social Security numbers, for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

340. Identity thieves can also use Social Security numbers to obtain a driver's license or other 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, seek unemployment or other benefits, and may even give the victim's PII and PHI to police during an arrest, resulting in an arrest warrant being issued in the victim's name.

---

[57] Albert Khoury, *Scam alert: 5 most costly data breaches (plus 5 states most targeted)* (July 27, 2022), https://www.komando.com/security-privacy/most-costly-data-breaches/847800/

[58] *PII and PHI: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf [https://perma.cc/GCA5-WYA5].

[59] *Identity Theft Recovery Steps*, FTC, https://www.identitytheft.gov/Steps [https://perma.cc/ME45-5N3A].

341. A study by the Identity Theft Resource Center ("ITRC") found that 96.7% of identity theft victims experienced costs and/or other harms from the criminal activity.[60] This includes devastating results, such as "I lost my home/place of residence" and "I couldn't care for my family." Moreover, the harms of identity theft are not limited to the affected individual and may adversely impact other associated persons and support systems, including government assistance programs. In the ITRC study, nearly one third of survey respondents had to request government assistance as a result of the identity theft, such as welfare, EBT, food stamps, or similar support systems.[61] The ITRC study concludes that "identity theft victimization has an extreme and adverse effect on each individual as well as all of the support systems and people associated with the individual."[62]

342. The PII and PHI exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiffs and Class Members at a higher risk of "phishing," "vishing," "smishing," and "pharming," [63]which are other ways for cybercriminals to exploit information they already have in order to get even more personally identifying information from a person through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

---

[60] Jason Steele, *Credit Card and ID Theft Statistics*, Creditcards.com (updated Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php [https://web.archive.org/web/20171215215318/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php].

[61] *Id.*

[62] *Id.*

[63] Phishing is the fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers; Vishing is the fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers; Smishing is the fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers; and Pharming is the fraudulent practice of directing internet users to a bogus website that mimics the appearance of a legitimate one, in order to obtain personal information such as passwords, account numbers, etc.

343. Personal Information, such as PII and PHI, 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.

344. 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 between when PII and PHI and/or financial information is stolen and when it is used. According to the GAO, 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.[64]

345. Personal Information, such as PII and PHI, is such an inherently valuable commodity to identity thieves that, once compromised, criminals often trade the information on the cyber black-market for years.

346. Furthermore, data breaches that expose any personal data, and in particular non-public data of any kind (*e.g.*, donation history or hospital records), directly and materially increase the chance that a potential victim is targeted by a spear phishing attack in the future, and spear phishing results in a high rate of identity theft, fraud, and extortion.[65]

347. There is a strong probability that entire batches of stolen information from the Data Breach have yet to be made available on the black market, meaning Plaintiffs and Class Members

---

[64] GAO Report, supra n. , at 29.

[65] *See* Kelion & Tidy, *supra* (concluding that personal information such as "names, titles, telephone numbers, email addresses, mailing addresses, dates of birth, and, more importantly, donor information such as donation dates, donation amounts, giving capacity, philanthropic interests, and other donor profile information . . . . in the hands of fraudsters, [makes consumers] particularly susceptible to spear phishing—a fraudulent email to specific targets while purporting to be a trusted sender, with the aim of convincing victims to hand over information or money or infecting devices with malware").

are at an increased risk of fraud and identity theft for many years into the future. Indeed, some of the Plaintiffs and many Class Members are in very early stages of their lives—in their twenties and thirties. Thus, as the Notice advises, Plaintiffs must vigilantly monitor their financial accounts for many years to come.

348. Defendants are highly sophisticated entities that regularly handle sensitive PII and PHI, yet they failed to establish and/or implement appropriate administrative, technical, and/or physical safeguards to ensure the security and confidentiality of Plaintiffs' and other Class Members' PII and PHI to protect against anticipated threats of intrusion of such information.

349. The ramifications of Defendants' failure to keep Plaintiffs' and Class Members' PII and PHI secure are long lasting and severe. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

350. Defendants knew, or should have known, the importance of safeguarding the PII and PHI entrusted to them and of the foreseeable consequences if their systems and/or those their vendors and HIPAA business associates, including NationsBenefits, were breached. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

351. Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

G. Defendants Caused Reasonably Foreseeable Harm to Plaintiffs and Class Members.

352. Charged with handling highly sensitive PII and PHI including healthcare information, financial information, and insurance information, Defendants knew or should have known the importance of safeguarding the PII and PHI that was entrusted to it. Defendants also knew or should have known of the foreseeable consequences if their vendors' and business associates' data security systems were breached. This includes the significant costs that would be imposed on Plaintiffs and the Class Members as a result of a breach. Defendants nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

353. Because of the highly sensitive and personal nature of the information Defendants acquire and store, Defendants knew or reasonably should have known that it stored protected PII and PHI and transmitted that data to vendors and business associates and must comply with healthcare industry standards related to data security and all federal and state laws protecting customers' and patients' PII and PHI and provide adequate notice to customers if their PII or PHI is disclosed without proper authorization.

354. By obtaining, collecting, receiving, storing, and/or transmitting Plaintiffs' and Class Members' PII and PHI, Defendants assumed legal and equitable duties and knew, or should have known, that it was thereafter responsible for protecting Plaintiffs' and Class Members' PII and PHI from unauthorized disclosure.

355. Defendants could have prevented or mitigated the effects of the Data Breach by better selecting and verifying, supervising, and auditing its HIPAA business associates.

356. As a result of Defendants' deficient security and monitoring measures, Plaintiffs and Class Members have been harmed by the compromise of their sensitive personal information,

which is currently for sale on the dark web and through private sale to other cyber criminals and/or being used by criminals for identify theft and other fraud-related crimes.

357. Plaintiffs and Class Members face a substantial and imminent risk of fraud and identity theft as their names have now been linked with their Social Security numbers, bank account numbers, emails, phone numbers, and physical addresses as a result of the Data Breach. These specific types of information are associated with a high risk of fraud.

358. Plaintiffs and Class Members also suffered a "deprivation of value" of their sensitive Personal Information when it was stolen by hackers in the Data Breach. A robust market exists for stolen personal information. Hackers sell personal information on the dark web—an underground market for illicit activity, including the purchase of hacked personal information—at specific identifiable prices. This market serves to determine the loss of value to Plaintiffs and Class Members.

359. As discussed above, Plaintiffs' and Class Members' stolen Personal Information is a valuable commodity to identity thieves.

360. Identity thieves can also combine data stolen in the Data Breach with other information about Plaintiffs and Class Members gathered from underground sources, public sources, or even Plaintiffs' and Class Members' social media accounts. Thieves can use the combined data to send highly targeted phishing emails to Plaintiffs and Class Members to obtain more sensitive information. Thieves can use the combined data to commit potential crimes, including opening new financial accounts in Plaintiffs' and Class Members' names, taking out loans in Plaintiffs' and Class Members' names, using Plaintiffs' and Class Members' information to obtain government benefits, filing fraudulent tax returns using Plaintiffs' and Class Members'

information, obtaining Social Security numbers in Plaintiffs' and Class Members' names but with another person's photograph, and giving false information to police during an arrest.

361. Plaintiffs and Class Members also suffered "benefit of the bargain" damages. Plaintiffs and Class Members overpaid for services that should have been—but were not—accompanied by adequate data security. Part of the premiums paid by Plaintiffs and Class Members to Defendants was intended to be used to fund adequate data security, including verifying, monitoring, and auditing that its HIPAA business associates maintained adequate security measures. Plaintiffs and Class Members did not get what they paid for.

362. Plaintiffs and Class Members have spent and will continue to spend substantial amounts of time monitoring their accounts for identity theft and fraud, the opening of fraudulent accounts, disputing fraudulent transactions, and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach.

363. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[66]

364. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[67] leisure time is defined as time not occupied with work or chores and is "the time equivalent of

[66] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour; *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data,* https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm%23type=1&year=2021&qtr=3&own=5 &ind=10&supp=0 (finding that on average, private-sector workers make $1,253 per 40-hour work week).

[67] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019).

'disposable income.'"[68] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

365. Plaintiffs and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

366. Plaintiffs and Class Members may also incur out of pocket costs for protective measures such as identity theft protection, credit monitoring fees, credit report fees, credit freeze fees, fees for replacement cards, and similar costs related to the Data Breach.

367. Class Members who experience actual identity theft and fraud will also be harmed by the inability to use their credit or debit cards when their accounts are suspended or otherwise rendered unusable due to fraudulent charges. To the extent Class Members are charged monthly/annual fees for their credit and/or debit accounts, they are left without the benefit of that bargain while they await receipt of their replacement cards. Class Members will be harmed further by the loss of rewards points or airline mileage that they cannot accrue while awaiting replacement cards. The inability to use payment cards may also result in missed payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations.

368. In the case of a data breach, merely reimbursing a consumer for a financial loss due to identity theft or fraud does not make that individual whole again. On the contrary, after

[68] *Id.*

conducting a study, the Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems."

369. A victim whose personal information has been stolen or compromised may not see the full extent of identity theft or fraud until long after the initial breach. Additionally, a victim whose personal information has been stolen may not become aware of charges when they are nominal, as typical fraud-prevention algorithms may not capture such charges. Those charges may be repeated, over and over again, on a victim's account.

370. The risk of identity theft and fraud will persist for years. Identity thieves often hold stolen data for months or years before using it to avoid detection. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because the data is often sold in small batches to various individuals rather than in bulk to a single buyer. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts *ad infinitum*.

V. CLASS ACTION ALLEGATIONS

371. Pursuant to Fed. R. Civ. P. 23(b)(2) and 23(b)(3), as applicable, and 23(c)(4), Plaintiffs seek certification of the following nationwide class (the "Class" or the "Nationwide Class") of similarly situated persons:

> All of Defendant's patients and customers whose PII and/or PHI was compromised in the Data Breach.

372. Pursuant to Fed. R. Civ. P. 23(b)(2) and 23(b)(3), as applicable, and 23(c)(4): the Aetna Plaintiffs seek certification of state common law claims in the alternative to the nationwide claims as well as statutory claims under state data breach notification and consumer protection and privacy statutes on behalf of residents of Connecticut, Florida, Georgia, Illinois, Kansas, Massachusetts, Michigan, Nevada, New York, North Carolina, North Dakota, Ohio, and

Oklahoma; the SCFHP Plaintiffs seek certification of state common law claims in the alternative to the nationwide claims as well as statutory claims under state data breach notification and consumer protection and privacy statutes on behalf of residents of California; Plaintiff Shepherd seeks certification of Indiana state common law claims in the alternative to the nationwide claims as well as statutory claims under Indiana data breach notification and consumer protection and privacy statutes on behalf of residents of Indiana; and Plaintiff Marshall seeks certification of Kentucky common law claims in the alternative to the nationwide claims as well as statutory claims under Kentucky data breach notification and consumer protection and privacy statutes on behalf of residents of Kentucky (collectively, the "Subclasses").

373. Each Subclass is defined as follows:

California Subclass: All SCFHP customers residing in California whose PII and/or PHI was compromised in the Data Breach

Connecticut Subclass: All Aetna customers residing in Connecticut whose PII and/or PHI was compromised in the Data Breach.

Florida Subclass: All Aetna customers residing in Florida whose PII and/or PHI was compromised in the Data Breach.

Georgia Subclass: All Aetna customers residing in Georgia whose PII and/or PHI was compromised in the Data Breach.

Illinois Subclass: All Aetna customers residing in Illinois whose PII and/or PHI was compromised in the Data Breach.

Indiana Subclass: All Anthem customers residing in Indiana whose PHI and/or PII was compromised in the Data Breach.

Kansas Subclass: All Aetna customers residing in Kansas whose PII and/or PHI was compromised in the Data Breach.

Kentucky Subclass: All Elevance customers residing in Indiana whose PII and/or PHI was compromised in the Data Breach

Massachusetts Subclass: All Aetna customers residing in Massachusetts whose PII and/or PHI was compromised in the Data Breach.

Michigan Subclass: All Aetna customers residing in Michigan whose PII and/or PHI was compromised in the Data Breach.

Nevada Subclass: All Aetna customers residing in Nevada whose PII and/or PHI was compromised in the Data Breach.

New York Subclass: All Aetna customers residing in New York whose PII and/or PHI was compromised in the Data Breach.

North Carolina Subclass: All Aetna customers residing in North Carolina whose PII and/or PHI was compromised in the Data Breach.

North Dakota Subclass: All Aetna customers residing in North Dakota whose PII and/or PHI was compromised in the Data Breach.

Ohio Subclass: All Aetna customers residing in Ohio whose PII and/or PHI was compromised in the Data Breach.

Oklahoma Subclass: All Aetna customers residing in Oklahoma whose PII and/or PHI was compromised in the Data Breach.

374. The Nationwide Class and Subclasses are collectively referred to as the Class or Classes.

375. Excluded from the Classes are: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendants and their subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which its parent has a controlling interest, and their respective current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Classes; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendants' counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

376. Plaintiffs reserve the right to amend or modify the Class definitions with greater specificity after having had the opportunity to conduct discovery.

377. **Numerosity**. Consistent with Rule 23(a)(1), the members of the Classes are so numerous and geographically dispersed that the joinder is impractical. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Classes consist of over one million individuals whose PII and PHI were compromised as a result of the Data Breach. Those persons' names and addresses are available from Defendants' records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include electronic mail, U.S. Mail, internet notice, and/or published notice. Upon information and belief, there are at least thousands of members in each Subclass, making joinder of all Subclass Members impractical.

378. **Commonality**. Rule 23(a)(2)'s commonality requirement is satisfied. There are many questions of law and fact common to each of the Classes. These common questions predominate over any individualized questions of individual Class and Subclass Members. These common questions of law and fact include, without limitation:

a. Whether Defendants owed a duty to Class and Subclass Members to safeguard their PII and PHI;

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

c. Whether Defendants' conduct violated the FTC Act or HIPAA;

d. Whether Defendants' data security systems and monitoring processes prior to and during the Data Breach complied with applicable data security laws and regulations, including HIPAA and HITECH;

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

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

g. Whether Defendants knew or should have known NationsBenefits' network and systems were susceptible to a data breach;

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

i. Whether Defendants were negligent in failing to adequately monitor and audit the data security systems of their HIPAA business associate NationsBenefits;

j. Whether Defendants' efforts (or lack thereof) to ensure the security of insureds' Personal Information provided to HIPAA business associates, such as NationsBenefits, were reasonable in light of known legal requirements.

k. Whether an implied contract existed between Class and Subclass Members and Defendants, providing that Defendants would implement and maintain reasonable security measures to protect and secure Class and Subclass Members' PII and PHI from unauthorized access and disclosure;

l. Whether Defendants breached implied contracts with Plaintiffs and Class and Subclass Members;

m. Whether Defendants was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class and Subclass Members;

n. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class and Subclass Members;

o. Whether Defendants owed a duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class and Subclass Members;

p. Whether Defendants failed to notify Plaintiffs and Class and Subclass Members as soon as practicable and without delay after the Data Breach was discovered;

q. Whether Defendants' delay in informing Plaintiffs and Class and Subclass Members of the Data Breach was unreasonable;

r. Whether Defendants' method of informing Plaintiffs and Class and Subclass Members of the Data Breach was unreasonable;

s. Whether Defendants' conduct, including its failure to act, resulted in or was the proximate cause of the loss of the PII and PHI of Plaintiffs and Class and Subclass Members;

t. Whether Plaintiffs and Class and Subclass Members were injured and suffered damages or other losses because of Defendants' failure to reasonably protect their PII and PHI; and

u. Whether, as a result of Defendants' conduct, Plaintiffs and Class and Subclass Members are entitled to damages, civil penalties, punitive damages, treble damages, nominal damages, or injunctive relief.

379. **Typicality**. Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other Class and Subclass Members because Plaintiffs' PII and PHI, like that of every other Class

and Subclass Member, was compromised in the Data Breach. Moreover, all Plaintiffs and Class and Subclass Members were subjected to Defendants' uniform negligent, unjust, deceptive, unfair, and improper conduct.

380. **Adequacy of Representation**. Consistent with Rule 23(a)(4), Plaintiffs are adequate Class and Subclass representatives because they are members of the Classes and their interests do not conflict with the interests of other Class and Subclass Members that they seek to represent. Plaintiffs are committed to pursuing this matter for the Classes with each Class's collective best interest in mind. Plaintiffs have retained counsel competent and experienced in complex class action litigation of this type and Plaintiffs intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the Class's and Subclasses' interests.

381. **Predominance**. Consistent with Rule 23(b)(3), Defendants have engaged in a common course of conduct toward Plaintiffs and Class and Subclass Members, in that all the Plaintiffs and Class and Subclass Members' PII and PHI was unlawfully and inadequately protected in the same way. The common issues arising from Defendants' conduct affecting Class and Subclass 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.

382. **Superiority**. Consistent with Rule 23(b)(3), 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 and Subclass 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 and Subclass Members would create a risk of

inconsistent or varying adjudications with respect to individual Class and Subclass 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, the parties' resources, and protects the rights of each Class and Subclass Member. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class and Subclass Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

383. The Classes defined above are readily ascertainable from information in Defendants' and NationsBenefits' possession. The Class and Subclasses consist of individuals who received services from Defendants. Thus, identification of the members of the Classes will be reliable and administratively feasible, and adequate notice can be given to Class and Subclass Members directly using information maintained in Defendants' records.

384. Defendants, through their uniform conduct, acted on grounds that apply generally to the Class and each Subclass as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis. Injunctive relief is necessary to uniformly protect the Classes' data. Plaintiffs seek prospective injunctive relief as a wholly separate remedy from any monetary relief.

385. Likewise, particular issues under Rule 23(c)(4) 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 owed a legal duty to Plaintiffs and the Classes to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Defendants failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiffs and the Class Members;

c. Whether Defendants failed to adequately monitor and audit the data security systems of their HIPAA business associates, like NationsBenefits;

d. Whether Defendants was unfairly and unjustly enriched as a result of its improper conduct, such that it would be inequitable for Defendants to retain the benefits conferred upon them by Plaintiffs and the other Class Members;

e. Whether adherence to HIPAA regulations, FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the disclosure of Plaintiffs' and Class and Subclass Members' Personal Information.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, Plaintiffs and the Subclasses and Against All Defendants)

386. Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1 through 385 above as if fully set forth herein.

387. Defendants required Plaintiffs and Class Members to provide their PII and PHI in order to obtain Defendants' services, specifically health care, health insurance and related benefits. Defendants collected, maintained, and stored Plaintiffs' and Class Members' PII and PHI and used it as well as shared and transmitted it to NationsBenefits for commercial gain.

388. Defendants had a non-delegable duty to ensure that NationsBenefits, as a contractual partners with whom it shared Plaintiffs' and Class Members' PII and PHI, maintained

adequate and commercially reasonable data security practices to ensure the protection of Plaintiffs' and Class Members' PII and PHI.

389. Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' PII and PHI in its control from being compromised, lost, stolen accessed and misused by unauthorized persons.

390. Defendants' duty included a responsibility to implement processes by which it could either detect a data breach of this type and magnitude in a timely manner or audit and verify the computer, network, and data security measures of NationsBenefits, which Defendants allowed to access Plaintiffs' and Class Members' PII and PHI.

391. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other statutory requirements, regulations, and other notices described above to ensure that NationsBenefits' systems and networks adequately protected Plaintiffs' and Class Members' PHI and PHI.

392. Defendants' duty of care arose as a result of the special relationship that existed between Defendants and Plaintiffs and Class Members. The special relationship arose because Plaintiffs and Class Members entrusted Defendants with their confidential data as part of the health care and health insurance processes. Only Defendants were in a position to ensure that their contractual partners had sufficient safeguards to protect against the foreseeable risk that a data breach could occur and would result in substantial harm to Plaintiffs and Class Members.

393. Defendants' duty to use reasonable care in protecting Personal Information arose as a result of the common law and the statutes and regulations, as well as its own promises regarding privacy and data security to Plaintiffs' and Class Members. This duty exists because

Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. By collecting and maintaining personal and confidential information of Plaintiffs and Class Members, and acknowledging that this information needed to be kept secure, it was foreseeable that they would be harmed in the future if Defendants did not protect Plaintiffs' and Class Members' information from threat actors.

394. Defendants' duty also arose under HIPAA regulations, which, as described above, applied to Defendants and establish national standards for the protection of patient information, including protected health information, which required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The duty also arose under HIPAA's Privacy rule requirement that Defendants obtain satisfactory assurances from their HIPAA business associate NationsBenefits that NationsBenefits would appropriately safeguard the protected health information it receives or creates on behalf of Defendants. 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

395. Defendants' duties also arose under Section 5 of the FTC 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 personal and confidential information. Various FTC publications and data security breach orders further form the basis of Defendants' duty. In addition, several individual states have enacted statutes based upon the FTC Act that also created a duty.

396. Defendants were subject to an "independent duty" untethered to any contract between Plaintiffs and Class Members and Defendants.

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

398. Defendants owed Plaintiffs and Class Members a duty to notify them within a reasonable time frame of any breach to their PII and PHI. Defendants 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 necessary for Plaintiffs and Class Members to take appropriate measures to protect their PII and PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of the Data Breach.

399. Defendants owed these duties to Plaintiffs 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 its inadequate security protocols. After all, Defendants actively sought and obtained the PII and PHI of Plaintiffs and Class Members.

400. Given the vast amount of highly valuable PII and PHI that Defendants aggregate and make available to third parties, like NationsBenefits, the risk that unauthorized persons would attempt to gain access to Plaintiffs' and Class Members' PII and PHI and misuse it was foreseeable. Defendants knew or should have known the importance of exercising reasonable care in handling the PII and PHI entrusted to it, including when allowing third parties like NationsBenefits access to Plaintiffs' and Class Members' sensitive PII and PHI.

401. Given the nature of Defendants' business, the sensitivity and value of the PII and PHI they maintain, and the resources at their disposal, Defendants should have identified and

foreseen that the third parties they share information with could have vulnerabilities in their systems and prevented the dissemination of Plaintiffs' and Class Members' PII/PHI.

402. It was or should have been reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII and PHI by failing to ensure that the third parties their share PII and PHI with design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII/PHI to unauthorized individuals.

403. It was also foreseeable that Defendants' failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and Class Members.

404. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII and PHI. And but for Defendants negligence, Plaintiffs and Class Members would not have been injured. The specific negligent acts and omissions committed by Defendants include, but are not limited to:

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

b. Failing to comply with—and thus violating—HIPAA and its regulations;

c. Failing to comply with—and thus violating—HITECH and its regulations;

d. Failing to comply with—and thus violating—FTC Act and its regulations;

e. Failing to adequately monitor the security of their and their HIPAA business associates' networks and systems;

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

g. Allowing unauthorized access to Class Members' PII and PHI;

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

i. 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.

405. It was foreseeable that Defendants failure to use reasonable measures to protect Class Members' PII and PHI would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII and PHI would result in one or more types of injuries to Class Members.

406. Defendants breached its duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII/PHI by failing to monitor, audit, evaluate, and ensure that the third parties it shares PII/PHI with design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems sufficient to safeguard and protect PII/PHI entrusted to them—including Plaintiffs' and Class members' PII/PHI. Defendants also failed to provide timely and adequately detailed notice of the Data Breach and that Plaintiffs' and Class Members' PII and PHI had been compromised.

407. Plaintiffs and Class Members had and have no ability to protect their PII/PHI that was, or remains, in Defendants' possession and control.

408. But for Defendants' negligent conduct or breach of the above-described duties, Plaintiffs' and Class Members' PII/PHI would not have been compromised. The PII/PHI of Plaintiffs and the Class was accessed and stolen as the proximate result of Defendants' failure to exercise reasonable care in safeguarding, securing, and protecting such PII and PHI by, *inter alia*, monitoring, auditing, and ensuring that third parties it contracts with and shares PII and PHI will adopt, implement, and maintain appropriate security measures and otherwise comply with HIPAA.

409. Defendants' failure to take proper security measures and to monitor, audit, and ensure that their third-party vendors and HIPAA business associates took proper security measures to protect sensitive Personal Information of Plaintiffs and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and Class Members' Personal Information.

410. Neither Plaintiffs nor the other Class Members contributed to the Data Breach and subsequent misuse of their PII and PHI.

411. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (a) a substantially increased and imminent risk of identity theft; (b) the compromise, publication, and theft of their PII and PHI; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII and PHI; (d) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (e) the continued risk to their PII and PHI which remains in Defendants' and NationsBenefits' possession; (f) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII and PHI compromised as a result of

the Data Breach; (g) overpayment for the services that were received without adequate data security; and (h) emotional distress directly and proximately caused by Defendants' negligence.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, Plaintiffs and the Subclasses and Against All Defendants)

412. Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1 through 385 above as if fully set forth herein.

413. Aetna is an entity covered by HIPAA (45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

414. Under HIPAA, Defendants have a duty to use reasonable security measures to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). HIPAA also requires Defendants to obtain satisfactory assurances beyond merely entering into a contract that its business associates would appropriately safeguard the protected health information it receives or creates on behalf of Defendants. 45 CFR § 164.502(e), 164.504(e), 164.532(d) and (e). Some or all of the information at issue in this case constitutes "protected health information" within the meaning of HIPAA. 45 C.F.R. § 164.530(c)(1). NationsBenefits constitutes a "business associate" within the meaning of HIPAA.

415. HIPAA further requires Defendants to disclose the unauthorized access and theft of the Personal Information to Plaintiffs and Class Members "without unreasonable delay" so that

Plaintiffs and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information. *See* 45 C.F.R. §§ 164.404, 406, 410. *See also* 42 U.S.C. § 17932.

416. Defendants violated HIPAA by failing to reasonably protect Plaintiffs' and Class Members' PII and PHI, as described herein.

417. Plaintiffs and Class Members are within the class of persons that the HIPAA was intended to protect. The harm Plaintiffs and Class Members have suffered and will suffer as a result of Defendants' breach of its duties is precisely the type of harm HIPAA is intended to guard against.

418. Under the FTC Act, Defendants have a duty to employ reasonable security measures. Specifically, this statute 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. 15 U.S.C. § 45(a)(1).

419. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

420. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Personal Information they obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving protected health information and companies as large as Defendants, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

421. Plaintiffs and Class Members are also within the class of persons that the FTC Act was intended to protect. Moreover, the harm Plaintiffs and Class Members have suffered and will

suffer as a result of Defendants' breach of their duties is precisely the type of harm the FTC Act is intended to guard against. 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 very same injuries that Defendants inflicted upon Plaintiffs and Class Members.

422. Defendants' negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injuries-in-fact and damages. These injuries include, but are not limited to, the theft of their PII and PHI by criminals, improper disclosure of their PII and PHI, lost benefit of their bargain, deprivation in value of their PII and PHI, 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. Moreover, injuries-in-fact and damages are ongoing, imminent, and immediate.

423. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class Members are entitled to recover compensatory and consequential damages.

424. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (a) strengthen their data security systems and vendor risk management and monitoring procedures; (2) submit to future annual audits of those systems and monitoring procedures; and (3) continue to provide adequate credit monitoring to all Class Members for the remainders of their lives.

COUNT III
BREACH OF CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class, or alternatively, Plaintiffs and the Subclasses and Against All Defendants)

425. Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1 through 385 above as if fully set forth herein.

426. Defendants and Plaintiffs and Class Members entered into contracts wherein Defendants agreed to provide health care, health insurance, and related services to their patients and customers.

427. Upon information and belief, Defendants, either directly or by incorporating their respective privacy policies by reference, promised to safeguard, secure, and protect Plaintiffs' and Class Members' PII and PHI, promised to comply with all federal and state laws and regulations, including HIPAA, and promised to timely and accurately provide notification if Plaintiffs' and Class Members' PII and PHI had been breached, compromised, or stolen.

428. Plaintiffs and Class Members fully performed their obligations under the contracts.

429. Defendants breached their contracts when they failed to safeguard, secure, and protect the PII and PHI of Plaintiffs and Class Members by failing to verify, monitor, and audit NationsBenefits to ensure it had adequate measures to safeguard, secure, and protect Plaintiffs' and Class Members' PII and PHI.

430. Defendants breached the contracts they made with Plaintiffs and Class Members by failing to safeguard and protect their PHI/PII and by failing to provide timely and accurate notice to them that their PHI/PII was compromised as a result of the Data Breach.

431. Defendants further breached the contracts with Plaintiffs and Class Members by failing to comply with their promise to abide by HIPAA.

432. Defendants further breached the contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information Defendants created, received, maintained, and transmitted in violation of 45 CFR § 164.306(a)(1).

433. Defendants further breached the contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR § 164.308(a)(1).

434. Defendants further breached the contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR § 164.306(a)(2).

435. Defendants' failures to meet these promises constitute breaches of the contracts.

436. Furthermore, the failure to meet their confidentiality and privacy obligations resulted in Defendants providing services to Plaintiffs and Class Members that were of diminished value.

437. As a direct and proximate result of Defendants' breaches of their contracts, Plaintiffs and Class Members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, to ensure their personal and financial safety.

438. As a direct and proximate result of Defendants' above-described breaches of contract, Plaintiffs' and Class Members have suffered (and will continue to suffer): (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

439. As a direct and proximate result of Defendants' above-described breaches of contract, Plaintiffs and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, Plaintiffs and the Subclasses and Against All Defendants)

440. Plaintiffs re-allege and incorporate by the allegations in paragraphs 1 through 385 above as if fully set forth herein.

441. This cause of action is pled in the alternative to the breach of contract theory.

442. For years and continuing to today, Defendants' business models have depended upon patients and insureds entrusting them with their Personal Information. Trust and confidence are critical and central to the services provided by Defendants. Unbeknownst to Plaintiffs and Class Members, however, Defendants failed to ensure their vendors and HIPAA business associates reasonably or adequately secured, safeguarded, and otherwise protected Plaintiffs' and Class Members' Personal Information. Defendants' deficiencies described herein were contrary to their security messaging.

443. Plaintiffs and Class Members engaged Defendants for health insurance and other benefits and provided Defendants with, and allowed Defendants to collect, their Personal Information on the mistaken belief that Defendants complied with their duty to safeguard and protect insureds' Personal Information. Putting their short-term profit ahead of safeguarding Personal Information, and unbeknownst to Plaintiffs and Class Members, Defendants knowingly sacrificed security in favor of collecting moneys Defendants believed they were owed. Defendants knew that the manner in which they maintained and transmitted patients' and customers' Personal Information violated their fundamental duties to Plaintiffs and Class Members by disregarding industry-standard security protocols to ensure confidential information was securely transmitted and stored.

444. Defendants had within their exclusive knowledge at all relevant times the fact that their vendors and HIPAA business associates failed to implement adequate security measures to keep patients' and insureds' Personal Information secure. This information was not available to Plaintiffs, Class Members, or the public at large.

445. Defendants also knew that Plaintiffs and Class Members expected that their information would be kept secure against known security risks and that the security protocols of any vendors or HIPAA business associates used by Defendants would be thoroughly vetted before they received Plaintiffs' and Class Members' Personal Information. And based on this expectation and trust, Defendants knew that Plaintiffs and Class Members would not have disclosed health or other sensitive information to them and would have chosen different providers for services.

446. Plaintiffs and Class Members did not expect that Defendants would store or transmit their Personal Information insecurely or engage another benefits provider, NationsBenefits, that employed substantially deficient security protocols and would store sensitive PHI and PII.

447. Plaintiffs and Class Members conferred a monetary benefit on Defendants by paying money for healthcare benefits and other services, a portion of which was intended to have been used by Defendants for data security measures to ensure the security of Plaintiffs' and Class Members' PII and PHI, including by monitoring and auditing NationsBenefits' networks and data security measures. Plaintiffs and Class Members further conferred a benefit on Defendants by entrusting their PII and PHI to Defendants from which Defendants derived profits.

448. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants

instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by avoiding their network and data security monitoring and auditing measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to ensure adequate security.

449. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendants failed to implement appropriate data security measures that are mandated by industry standards, including monitoring and auditing NationsBenefits' network and data security measures.

450. Defendants acquired the monetary benefit, PII, and PHI through inequitable means in that Defendants failed to disclose the inadequate security practices, previously alleged, and failed to ensure NationsBenefits maintained adequate data security measures.

451. Had Plaintiffs and Class Members known about Defendants' practice of sharing their Personal Information with vendors and HIPAA business associates who were unequipped to protect it and insecurely transmitting sensitive PII and PHI that had no legitimate business need for it, Plaintiffs and Class Members would not have engaged Defendants to provide health care, health insurance benefits and other related services and would never have provided Defendants with their Personal Information.

452. By withholding these material facts, Defendants put their own interests ahead of their insureds' interests and benefitted themselves to the detriment of Plaintiffs and Class Members.

453. As a result of its conduct as alleged herein, Defendants sold more health insurance and other services than they otherwise would have and were able to charge Plaintiffs and Class

Members when they otherwise could not have. Defendants were unjustly enriched by charging for and collecting those benefits and other services to the detriment of Plaintiffs and Class Members.

454. Defendants' defective security and their unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their private Personal Information.

455. Plaintiffs and Class Members have no adequate remedy at law.

456. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered—and will continue to suffer—a host of injuries, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity to determine how their PII and PHI is used; (c) the compromise, publication, or theft of their PII and PHI; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, or unauthorized use of their PII and PHI; (e) 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; (f) the continued risk to their PII and PHI, 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 the PII and PHI in their possession; and (g) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach.

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

458. Defendants 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 Plaintiffs and Class Members.

COUNT V
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, Plaintiffs and the Subclasses and Against All Defendants)

459. Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1 through 385 above as if fully set forth herein.

460. Plaintiffs and Class Members maintained a confidential relationship with Defendants whereby Defendants undertook a duty not to disclose the PII and PHI provided by Plaintiffs and Class Members to Defendants to unauthorized third parties. Such PII and PHI was confidential and immutable, highly personal and sensitive, and not generally known.

461. Defendants knew Plaintiffs' and Class Members' PII and PHI was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the Personal Information they collected, stored, and maintained.

462. Defendants affirmatively disclosed Plaintiffs' and Class Members' PII and PHI to NationsBenefits without their consent and without any legitimate business need.

463. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiffs' and Class Members' PII and PHI. The unauthorized disclosure occurred because Defendants: (a) disclosed the PII and PHI to NationsBenefits without a legitimate business reason to do so and without consent; and (b) failed to implement and maintain reasonable safeguards to protect the PII and PHI in Defendants' possession and failed to comply with industry-standard data security practices.

464. NationsBenefits did not need access to Plaintiffs' and Class Members' PII and PHI at all unless and until they actually decided to obtain NationsBenefits' services. But Defendants nevertheless regularly and affirmatively provided full account information that included PII and PHI, apparently because it was more expedient than waiting until a member actually wanted to obtain NationsBenefits' services.

465. Plaintiffs and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

466. As a direct and proximate result of Defendants' breach of confidence, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT VI
REQUEST FOR EQUITABLE RELIEF
UNDER THE DECLARATORY JUDGMENT ACT
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, Plaintiffs and the Subclasses and Against All Defendants)

467. Plaintiffs re-allege and incorporate by reference the allegations in paragraphs 1 through 385 above as if fully set forth herein.

468. 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 grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

469. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard their patients' and customers' Personal Information and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches

that compromise their Personal Information. Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their Personal Information and remain at imminent risk that further compromises of their Personal Information will occur in the future given the publicity around the Data Breach and the nature and quantity of the Personal Information stored by Defendants and transmitted by Defendants to NationsBenefits.

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

a. Defendants continue to owe a legal duty to secure members' Personal Information and to timely notify members of a data breach under the common law, HIPAA, Section 5 of the FTC Act, and various state statutes; and

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure members' Personal Information, including to monitor, oversee, and audit their HIPAA business associates' compliance with HIPAA.

471. The Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect Plaintiffs' and Class members' Personal Information.

472. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach similar to the Data Breach at issue here. The risk of another data breach is real, immediate, and substantial. If another data breach occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

473. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Among other things, if another massive data breach occurs, Plaintiffs and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants has a pre-existing legal obligation to employ such measures.

474. 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 at Defendants or Defendants' HIPAA business associates, thus eliminating the additional injuries that would result to Plaintiffs, Class Members, and the millions of Defendants' patients and customers whose confidential information would be further compromised.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT VII
CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code §§ 1798.100 *et seq.*
(On Behalf of Plaintiffs Skurauskis, R. Rogers, N. Rogers and the California Subclass and Against SCFHP)

475. Plaintiffs Skurauskis, R. Rogers, N. Rogers ("SCFHP Plaintiffs") re-allege and incorporate by reference the allegations in paragraphs 1 through 385 above as if fully set forth herein.

476. SCFHP Plaintiffs bring this claim on behalf of themselves and the California Subclass.

477. SCFHP Plaintiffs and California Subclass Members are residents of California.

478. SCFHP is a corporation organized or operated for the profit or financial benefit of its owners. SCFHP collects consumers' Private Information (for the purposes of this section,

"Private Information") as defined in the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.140.

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

480. SCFHP has a duty to implement and maintain reasonable security procedures and practices to protect SCFHP Plaintiffs' and California Subclass Members' Private Information. As detailed herein, SCFHP failed to do so.

481. As a direct and proximate result of SCFHP's acts, SCFHP Plaintiffs' and California Subclass Members' Private Information, including names, contact information, dates of birth, health insurance information, and other sensitive medical records, was subjected to unauthorized access and exfiltration, theft, or disclosure.

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

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

484. SCFHP Plaintiffs and the California Subclass seek actual damages, as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

485. On June 23, 2023, counsel for SCFHP Plaintiffs provided written notice via certified mail to SCFHP at its principal place of business of the intent to pursue claims under the CCPA and an opportunity for SCFHP to cure. The domestic return receipt shows that SCFHP received the letter. SCFHP Plaintiffs' written notice set forth the violations of SCFHP's duty to implement and maintain reasonable security procedures and practices alleged in this Complaint.

486. To date, SCFHP has taken no action to remedy its misconduct or otherwise address the violations outlined in the written notice sent by Plaintiffs' counsel.

487. SCFHP Plaintiffs and the California Subclass seek actual damages, as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; reasonable attorneys' fees and costs; and statutory damages.

COUNT VIII
CALIFORNIA CONSUMER RECORDS ACT
Cal. Civ. Code §§ 1798.80 *et seq.*
(On Behalf of Plaintiffs Skurauskis, R. Rogers, N. Rogers and the California Subclass and Against SCFHP)

488. SCFHP Plaintiffs reallege and incorporate by reference the allegations in paragraphs 1 through 385 above, as if fully set forth herein.

489. SCFHP Plaintiffs bring this claim on behalf of themselves and the California Subclass.

490. "[T]o ensure that Private Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Private Information about a California resident shall implement and

maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Private Information from unauthorized access, destruction, use, modification, or disclosure."

491. SCFHP is a business that owns, maintains, and licenses Private Information (or "Private Information"), within the meaning of Cal. Civ. Code §§ 1798.80(a) and 1798.81.5(b), about Plaintiffs and California Subclass Members.

492. Businesses that own or license computerized data that includes Private Information are required to notify California residents when their Private Information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Private Information [Private Information] that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

493. SCFHP is a business that owns or licenses computerized data that includes "Private Information" [Personal Information] as defined by Cal. Civ. Code § 1798.80.

494. SCFHP Plaintiffs' and California Subclass Members' Private Information includes "Private Information" as covered by Cal. Civ. Code § 1798.82.

495. Because SCFHP reasonably believed that SCFHP Plaintiffs' and California Subclass Members' Private Information was acquired by unauthorized persons during the Data Breach, SCFHP had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

496. SCFHP failed to fully disclose material information about the Data Breach, including the types of Private Information impacted.

497. By failing to disclose the Data Breach in a timely and accurate manner, SCFHP violated Cal. Civ. Code § 1798.82.

498. SCFHP also violated Cal. Civ. Code § 1798.82 by not publishing a notice of data breach in the format required by Cal. Civ. Code § 1798.82(d)(1).

499. As a direct and proximate result of SCFHP's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, SCFHP Plaintiffs and California Subclass Members suffered damages, as alleged above.

500. SCFHP Plaintiffs and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT IX
CALIFORNIA UNFAIR COMPETITION ACT
Cal. Bus. & Prof. Code §§ 17200 *et seq*.
(On Behalf of Plaintiffs Skurauskis, R. Rogers, N. Rogers and the California Subclass and Against SCFHP)

501. SCFHP Plaintiffs reallege and incorporate by reference the allegations in paragraphs 1 through 385 above, as if fully set forth herein.

502. SCFHP Plaintiffs bring this claim on behalf of themselves and the California Subclass.

503. SCFHP is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

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

505. SCFHP's "unfair" acts and practices include:

a. SCFHP failed to implement and maintain reasonable security measures to protect SCFHP Plaintiffs' and California Subclass Members' Personal Information from

unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

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

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

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

506. SCFHP 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.

507. SCFHP's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures, including monitoring and overseeing its HIPAA business associate, to protect SCFHP Plaintiffs' and California Subclass Members' Personal 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 SCFHP Plaintiffs' and California Subclass Members' Personal 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 SCFHP Plaintiffs' and California Subclass Members' Personal 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 SCFHP Plaintiffs' and California Subclass Members' Personal 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 SCFHP Plaintiffs' and California Subclass Members' Personal 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 SCFHP Plaintiffs' and California Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, and § 1798.81.5, and California's Consumer Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq*, 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).

508. SCFHP's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of SCFHP's data security and ability to protect the confidentiality of consumers' Personal Information.

509. As a direct and proximate result of SCFHP's unfair, unlawful, and fraudulent acts and practices, SCFHP Plaintiffs and California Subclass Members were injured and suffered monetary and non-monetary damages, as alleged 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; deprivation of value of their Personal Information; overpayment for SCFHP's services; loss of the value of access to their Personal Information; and the value of identity protection services made necessary by the Data Breach.

COUNT X
CALIFORNIA CONSUMER LEGAL REMEDIES ACT
Cal. Civ. Code §§ 1750 *et seq*.
(On Behalf of Plaintiffs Skurauskis, R. Rogers, N. Rogers and the California Subclass and Against SCFHP)

510. SCFHP Plaintiffs reallege and incorporate by reference the allegations in paragraphs 1 through 385 above, as if fully set forth herein.

511. SCFHP Plaintiffs bring this claim on behalf of themselves and the California Subclass.

512. 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.

513. SCFHP is a "person" as defined by Civil Code §§ 1761(c) and 1770 and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

514. SCFHP Plaintiffs 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.

515. SCFHP's acts and practices were intended to and did result in the sales of products and services to SCFHP Plaintiffs 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.

516. SCFHP's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of SCFHP's data security and ability to protect the confidentiality of consumers' Personal Information.

517. Had SCFHP disclosed to SCFHP Plaintiffs and California Subclass Members that its HIPAA business associate's data systems were not secure and, thus, were vulnerable to attack, SCFHP would have been unable to continue sending PII and PHI to NationsBenefits and it would have been forced to adopt reasonable data security and vendor risk management measures and comply with the law. SCFHP was trusted with sensitive and valuable Personal Information regarding hundreds of thousands of individuals, including SCFHP Plaintiffs and California Subclass Members. SCFHP accepted the non-delegable responsibility of protecting the data but kept the inadequate state of its security controls secret from the public. Accordingly, SCFHP Plaintiffs and California Subclass Members acted reasonably in relying on SCFHP's misrepresentations and omissions, the truth of which they could not have discovered.

518. As a direct and proximate result of SCFHP's violations of California Civil Code § 1770, SCFHP Plaintiffs 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 Personal Information; overpayment for SCFHP's services; loss of the value of access to their Personal Information; and the value of identity protection

services made necessary by the Data Breach.

CLAIMS ON BEHALF OF THE CONNECTICUT SUBCLASS

COUNT XI
CONNECTICUT UNFAIR TRADE PRACTICES ACT
Conn. Gen. Stat. Ann. §§ 42-110a *et seq.*
(On Behalf of Plaintiff Titcomb and the Connecticut Subclass and Against Aetna)

519. Plaintiff Titcomb ("Plaintiff" for the purposes of this Count), individually and on behalf of the Connecticut Subclass, repeats and re-alleges all preceding allegations in paragraphs 1 through 385 as if fully set forth herein.

520. The Connecticut Unfair Trade Practices Act ("CUTPA") provides that "[n]o person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Conn. Gen. Stat. Ann. §42-110b(a). CUTPA expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the FTC Act. *See* Conn. Gen. Stat. Ann. §42-110b(b).

521. Aetna is a "person" as defined by Conn. Gen. Stat. Ann. §42-110a(3).

522. Plaintiff and Connecticut Subclass Members are actual consumers of Aetna's goods or services and qualify as a "person who suffers any ascertainable loss of money or property, real or personal, as a result of the use or employment of a method, act or practice prohibited by section 42-110b" under Conn. Gen. Stat. Ann. §42-110g.

523. Aetna advertised, offered, or sold goods or services in Connecticut and therefore engaged in trade or commerce directly or indirectly affecting the people of Connecticut. Conn. Gen. Stat. §42-110a(4).

524. Aetna engaged in deceptive, unfair, and unlawful acts and practices in the conduct of trade or commerce, in violation of CUTPA.

525. Aetna's deceptive acts and practices include:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Connecticut Subclass Members' PII and PHI;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Connecticut Subclass Members' PII and PHI, including duties imposed by the FTC Act, HIPAA, the Connecticut Insurance Information and Privacy Protection Act (Conn. Gen. Stat. Ann. §38a-988), and the Connecticut data breach notification statute (Conn. Gen. Stat. Ann. §42-471);

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Connecticut Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Connecticut Subclass Members' PII and PHI; and

d. 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 Connecticut Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Connecticut Insurance Information and Privacy Protection Act (Conn. Gen. Stat. Ann. §38a-988).

526. Aetna's unfair acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Connecticut Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiff's and

Connecticut Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiff's and Connecticut Subclass Members' PII and PHI;

b. Disclosing Plaintiff's and Connecticut Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Connecticut Subclass Members' PII and PHI, including duties imposed by the FTC Act, HIPAA, and the Connecticut Insurance Information and Privacy Protection Act (Conn. Gen. Stat. Ann. §38a-988); and

d. Failing to comply with the duties imposed by Conn. Gen. Stat. Ann. §36a-701b and disclose the Data Breach to Plaintiff and the Connecticut Subclass in a timely and accurate manner.

527. Aetna's conduct constitutes unfair methods of competition and unfair practices within the meaning of CUTPA because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Connecticut Subclass Members' PII and PHJI. Further, the injuries suffered by Plaintiff and the Connecticut Subclass Members are not outweighed by any countervailing benefits to consumers or competition. And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiff's and Connecticut Subclass Members' PII

and PHI, there is no way Plaintiff and the Connecticut Subclass Members could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the adequacy of its data security measures, Aetna created an asymmetry of information between it and the consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

528. Aetna's conduct constitutes unfair practices within the meaning of CUTPA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA, as well as the Connecticut Insurance Information and Privacy Protection Act (Conn. Gen. Stat. Ann. §38a-988).

529. Aetna's acts and practices are unfair because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with Aetna. Further, Aetna took reasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Aetna and consumers' inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

530. The above deceptive or unfair acts and practices by Aetna also violated Connecticut's Unfair Insurance Practices Act, Conn. Gen. Stat. Ann. §§38a-815, 816(1)-(2).

531. Aetna's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security measures and ability to protect the confidentiality of consumers' PII and PHI.

532. Aetna's acts and practices, including its material omissions, were likely to, and did in fact, deceive and mislead members of the public, including consumers acting reasonably under

the circumstances, to their detriment.

533. Aetna intended to mislead Plaintiff and Connecticut Subclass Members and induce them to rely on its misrepresentations and omissions.

534. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in their possession. This duty arose because members of the public, including Plaintiff and the Connecticut Subclass Members, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

535. Had Aetna disclosed to Plaintiff and the Connecticut Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna 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. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and the Connecticut Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Connecticut Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

536. Aetna acted intentionally, knowingly, and maliciously to violate CUTPA and recklessly disregarded Plaintiff's and Connecticut Subclass Members' rights.

537. Aetna's deceptive and unfair trade practices significantly impact the public, because many members of the public are actual or potential consumers of Aetna's services and the Data Breach affected millions of Americans, which include members of the Connecticut Subclass.

538. Aetna's violations present a continuing risk to Plaintiff and the Connecticut Subclass as well as to the general public.

539. As a direct and proximate result of Aetna's deceptive or unfair trade practices, Plaintiff and the Connecticut Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiff and Connecticut Subclass Members have suffered and will continue to suffer a range of injuries, including but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) 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; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

540. Plaintiff and the Connecticut Subclass seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, equitable relief, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS

COUNT XII
FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
Fla. Stat. §§501.201, et seq.
(On Behalf of Plaintiffs Luciano, Veazey and the Florida Subclass and Against Aetna)

541. Plaintiffs Luciano and Veazey ("Plaintiffs" for purposes of this Count), individually and on behalf of the Florida Subclass Members, repeat and re-allege all preceding allegations in paragraphs 1 through 385 as if fully set forth herein.

542. The Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. §§501.201, *et seq*., prohibits unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of trade or commerce. *See* Fla. Stat. §501.204(1). FDUTPA expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the FTC Act. *See* Fla. Stat. §501.204(2); *see also* Fla. Stat. §§501.202(3), 501.203(3)(a)-(c).

543. Plaintiffs and the Florida Subclass Members are "consumers" as defined by Fla. Stat. §501.203(7) and Plaintiffs and each Florida Subclass Member are aggrieved and have suffered a loss under Fla. Stat. §501.211(1)-(2) as a result of Aetna's violations of FDUTPA.

544. Aetna is engaged in a trade or commerce within the meaning of Fla. Stat. §501.203(8).

545. Aetna advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the citizens of Florida.

546. Plaintiffs and Florida Subclass Members are Aetna health plan holders located in Florida, where Aetna is authorized to do business. The conduct constituting Aetna's deceptive, unfair, and unconscionable acts and practices under this claim occurred primarily and substantially in Florida because Aetna is authorized to do business in Florida, and Aetna's unlawful conduct: (a) foreseeably impacted consumers residing in Florida whose PII and PHI was compromised in the Data Breach; and (b) otherwise interfered with trade or commerce in Florida.

547. Aetna engaged in unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of trade and commerce in violation of Fla. Stat. §501.204(1).

548. Aetna's deceptive acts and practices include:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Florida Subclass Members' PII and PHI;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Florida Information Protection Act (Fla. Stat. §501.171);

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Florida Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiffs' and Florida Subclass Members' PII and PHI; and

d. 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 Plaintiffs' and Florida Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Florida Information Protection Act (Fla. Stat. §501.171).

549. Aetna's unfair or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Florida Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiffs' and Florida Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiffs' and Florida Subclass Members' PII and PHI;

b. Disclosing Plaintiffs' and Florida Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA; and

d. Failing to comply with the duties imposed by the Florida Information Protection Act (Fla. Stat. §501.171) and disclose the Data Breach to Plaintiffs and the Florida Subclass Members in a timely and accurate manner.

550. Aetna's conduct constitutes unfair methods of competition or unfair or unconscionable practices within the meaning of FDUTPA because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiffs' and Florida Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiffs and the Florida Subclass Members are not outweighed by any countervailing benefits to consumers or competition. And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiffs' and Florida Subclass Members' PII and PHI, there is no way Plaintiffs and the Florida Subclass Members could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security, Aetna created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

551. Aetna's conduct constitutes unfair practices within the meaning of FDUTPA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA as well as the Florida Information Protection Act (Fla. Stat. §501.171).

552. Aetna's acts and practices are unfair or unconscionable because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with Aetna. Further, Aetna took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Aetna and consumers' inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

553. Aetna's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security measures and ability to protect the confidentiality of consumers' PII and PHI.

554. Aetna's acts and practices, including its material omissions, were likely to, and did in fact, deceive and mislead members of the public, including consumers acting reasonably under the circumstances, to their detriment.

555. Aetna intended to mislead Plaintiffs and Florida Subclass Members and induce them to rely on its misrepresentations and omissions.

556. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in their possession. This duty arose because members of the public, including Plaintiff and the Florida Subclass, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

557. Had Aetna disclosed to Plaintiff and the Florida Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna 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. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiffs and the Florida Subclass. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and the Florida Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

558. Aetna acted intentionally, knowingly, and maliciously to violate FDUTPA, and recklessly disregarded Plaintiffs' and Florida Subclass Members' rights.

559. Aetna's violations present a continuing risk to Plaintiffs and the Florida Subclass Members as well as to the general public.

560. As a direct and proximate result of Aetna's deceptive, unfair, or unconscionable acts and practices, Plaintiffs and the Florida Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiffs and Florida Subclass Members have suffered and will continue to suffer a range of injuries, including but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) 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; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

561. Plaintiff and the Florida Subclass seek all monetary and non-monetary relief allowed by law, including damages, equitable relief, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE GEORGIA SUBCLASS

COUNT XIII
GEORGIA UNIFORM DECEPTIVE PRACTICES ACT
Ga. Code. Ann. §§10-1-370, et seq.
(On Behalf of Plaintiff Peffley-Wilson and the Georgia Subclass and Against Aetna)

562. Plaintiff Peffley-Wilson ("Plaintiff" for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and re-alleges all preceding allegations in paragraphs 1 through 385 as if fully set forth herein.

563. Aetna, Plaintiff, and each member of the Georgia Subclass are "persons" within the meaning of Ga. Code Ann. §10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

564. Aetna engaged in deceptive trade practices in the conduct of its business, in violation of Ga. Code Ann. §10-1-372(a), including:

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 if they are of another;

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

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

565. Aetna's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Georgia Subclass Members' PII and PHI,

including by failing to properly secure and encrypt Plaintiff's and Georgia Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiff's and Georgia Subclass Members' PII and PHI;

b. Disclosing Plaintiff's and Georgia Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the Georgia Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Georgia Insurance Information and Privacy Protection Act (Ga. Code Ann. §33-39-14) and the Georgia Personal Identity Protection Act (Ga. Code Ann. §§10-1-910, *et seq*.);

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and the Georgia Subclass Members' PII and PHI;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the Georgia Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Georgia Insurance Information and Privacy Protection Act (Ga. Code Ann. §33-39-14) and the Georgia Personal Identity Protection Act (Ga. Code Ann. §§10-1-910, *et seq*.);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and the Georgia Subclass

Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Georgia Subclass Members' PII and PHI; and

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 the Georgia Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Georgia Insurance Information and Privacy Protection Act (Ga. Code Ann. §33-39-14) and the Georgia Personal Identity Protection Act (Ga. Code Ann. §§10-1-910, *et seq*.).

566. Aetna's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security and ability to protect the confidentiality of consumers' PII and PHI.

567. Aetna intended to mislead Plaintiff and the Georgia Subclass Members and induce them to rely on its misrepresentations and omissions.

568. In the course of its business, Aetna engaged in activities with a tendency or capacity to deceive.

569. Aetna acted intentionally, knowingly, and maliciously to violate Georgia's UDTPA, and recklessly disregarded Plaintiff's and the Georgia Subclass Members' rights.

570. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in its possession. This duty arose because members of the public, including Plaintiff and the Georgia Subclass Members, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its

possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

571. Had Aetna disclosed to Plaintiff and the Georgia Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna 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. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and the Georgia Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Georgia Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

572. Aetna's violations present a continuing risk to Plaintiff and the Georgia Subclass Members as well as to the general public.

573. As a direct and proximate result of Aetna's deceptive trade practices, Plaintiff and the Georgia Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiff and Georgia Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) 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; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

574. Plaintiff and the Georgia Subclass Members seek all relief allowed by law, including equitable relief and reasonable attorneys' fees and costs under Ga. Code Ann. § 10-1-373.

CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS

COUNT XIV
ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
Ill. Comp. Stat. §§505/1, et seq.
(On Behalf of Plaintiff Mueller and the Illinois Subclass and Against Aetna)

575. Plaintiff Mueller ("Plaintiff" for purposes of this Count), individually and on behalf of the Illinois Subclass Members, repeats and re-alleges all preceding allegations in paragraphs 1 through 385 as if fully set forth herein.

576. The Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA"), 815 Ill. Comp. Stat. §§ 505/1, *et seq.*, prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce. *See* 815 Ill. Comp. Stat. §505/2. ICFA expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the FTC Act. *See id*.

577. Plaintiff and the Illinois Subclass Members are a "person," as defined in 815 Ill. Comp. Stat. Ann. §505/1(c), are a "consumer," as defined in 815 Ill. Comp. Stat. Ann. §505/1(e), and satisfy the consumer nexus test in that Aetna's unfair and deceptive acts and practices were directed at and impacted the market generally and/or otherwise implicate consumer protection concerns where Aetna's unfair and deceptive acts and practices have impacted at least thousands of consumers in Illinois and millions nationwide and remedying Aetna's wrongdoing through the relief requested herein would serve the interests of consumers. Furthermore, Plaintiff and the Illinois Subclass Members are consumers located in Illinois, who obtained insurance and health benefits services from Aetna.

578. Aetna is a "person" as defined by 815 Ill. Comp. Stat. §505/1(c).

579. Aetna's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. §505/1(f).

580. Under ICFA the use or employment of any practice described in Section 2 of the Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. Ann. §510/2, in the conduct of any trade or commerce is unlawful whether any person has in fact been misled, deceived, or damaged thereby.

581. Aetna's deceptive acts and practices include:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Illinois Subclass Members' PII and PHI;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Illinois Insurance Information and Privacy Protection

Act (215 Ill. Comp. Stat. §5/1014), Illinois Personal Information Protection Act (815 Ill. Comp. Stat. §530/1, *et seq*., Illinois laws regulating the use and disclosure of Social Security Numbers (815 Ill. Comp. Stat. §505/2RR), and the Illinois Uniform Deceptive Trade Practices Act (815 Ill. Comp. Stat. §510/2(a));

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Illinois Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Illinois Subclass Members' PII and PHI; and

d. 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 Illinois Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Illinois Insurance Information and Privacy Protection Act (215 Ill. Comp. Stat. §5/1014), Illinois Personal Information Protection Act (815 Ill. Comp. Stat. §530/1, *et seq.*), Illinois laws regulating the use and disclosure of Social Security Numbers (815 Ill. Comp. Stat. §505/2RR), and the Illinois Uniform Deceptive Trade Practices Act (815 Ill. Comp. Stat. §510/2(a)).

582. Aetna's unfair acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Illinois Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiff's and Illinois

Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiff's and Illinois Subclass Members' PII and PHI;

b. Disclosing Plaintiff's and Illinois Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Illinois Insurance Information and Privacy Protection Act (215 Ill. Comp. Stat. §5/1014), Illinois Personal Information Protection Act (815 Ill. Comp. Stat. §530/1, *et seq.*), Illinois laws regulating the use and disclosure of Social Security Numbers (815 Ill. Comp. Stat. §505/2RR), and the Illinois Uniform Deceptive Trade Practices Act (815 Ill. Comp. Stat. §510/2(a)); and

d. Failing to comply with the duties imposed by 815 Ill. Comp. Stat. §530/10 and disclose the Data Breach to Plaintiff and the Illinois Subclass Members in a timely and accurate manner.

583. Aetna's conduct constitutes unfair methods of competition and unfair practices within the meaning of ICFA because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Illinois

Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiff and the Illinois Subclass Members are not outweighed by any countervailing benefits to consumers or competition. And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiff's and Illinois Subclass Members' PII and PHI, there is no way Plaintiff and the Illinois Subclass Members could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security, Aetna created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

584. Aetna's conduct constitutes unfair practices within the meaning of ICFA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA as well as the Illinois Insurance Information and Privacy Protection Act (215 Ill. Comp. Stat. §5/1014), Illinois Personal Information Protection Act (815 Ill. Comp. Stat. §530/1, *et seq*.), Illinois laws regulating the use and disclosure of Social Security Numbers (815 Ill. Comp. Stat. §505/2RR), and the Illinois Uniform Deceptive Trade Practices Act (815 Ill. Comp. Stat. §510/2(a)).

585. Aetna's acts and practices are unfair because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with Aetna. Further, Aetna took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Aetna and consumers' inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

586. Aetna's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security and ability to protect the confidentiality of consumers' PII and PHI.

587. Aetna's acts and practices, including its material omissions, were likely to, and did in fact, deceive and mislead members of the public, including consumers acting reasonably under the circumstances, to their detriment.

588. Aetna intended to mislead Plaintiff and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

589. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in their possession. This duty arose because members of the public, including Plaintiff and the Illinois Subclass Members, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

590. Had Aetna disclosed to Plaintiff and the Illinois Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna 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. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and the Illinois Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Illinois Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

591. Aetna acted intentionally, knowingly, and maliciously to violate ICFA, and recklessly disregarded Plaintiff's and Illinois Subclass Members' rights.

592. Aetna's violations present a continuing risk to Plaintiff and the Illinois Subclass Members as well as to the general public.

593. As a direct and proximate result of Aetna's unfair, unlawful, and deceptive trade practices, Plaintiff and the Illinois Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) 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; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in their possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

594. Plaintiff and the Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, equitable relief, and reasonable attorney's fees and costs.

CLAIMS ON BEHALF OF THE INDIANA SUBCLASS

COUNT XV
INDIANA DECEPTIVE CONSUMER SALES ACT
Ind. Code §§24-5-0.5-1, *et seq.*
(On Behalf of Plaintiff Shepard and the Indiana Subclass and Against Anthem)

595. Plaintiff Shepard ("Plaintiff" for purposes of this Count), individually and on behalf of the Indiana Subclass Members, repeats and re-alleges all preceding allegations in paragraphs 1 through 385 as if fully set forth herein.

596. Anthem, Plaintiff, and each member of the Indiana Subclass is a "person" as defined by Ind. Code §24-5-0.5-2(a)(2).

597. Anthem is a "supplier" as defined by §24-5-0.5-2(a)(1), because it regularly engages in or solicits "consumer transactions," within the meaning of §24-5-0.5-2(a)(3)(A).

598. Anthem's deceptive acts and practices include:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Indiana Subclass Member's PII and PHI;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of privacy of Plaintiff's and Indiana Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Ind. Code §4-1-11, *et seq*., and Ind. Code §24-4.9-1, *et seq*.

c. Omitting, suppressing and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Indiana Subclass Members'

PII and PHI including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Indiana Subclass Members' PII and PHI; and

d. 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 Indiana Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA, as well as Ind. Code §4-1-11, *et seq*., and Ind. Code §24-4.9-1, *et seq*.

599. Anthem's unfair or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Indiana Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiff's and Indiana Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiff's and Indiana Subclass Members' PII and PHI;

b. Disclosing Plaintiff's and Indiana Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Indiana Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPPA; and

d. Failing to comply with duties imposed by Ind. Code §4-1-11, *et seq*., and Ind. Code §24-4.9-1, *et seq*. and disclose the Data Breach to Plaintiff and

the Indiana Subclass Members in a timely and accurate manner.

600. Anthem's conduct constitutes unfair methods of competition or unfair or unconscionable practices within the meaning of the Indiana Deceptive Consumer Sales Act ("IDCSA") because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Anthem cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Indiana Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiff and the Indiana Subclass Members are not outweighed by any countervailing benefits to consumers or competition. And, because Anthem is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiff's and Indiana Subclass Members' PII and PHI, there is no way Plaintiff and the Indiana Subclass Members could have known about Anthem's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security, Anthem created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Anthem's legitimate business interests.

601. Anthem's conduct constitutes unfair practices within the meaning of IDCSA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA as well as Ind. Code §4-1-11, *et seq*., and Ind. Code §24-4.9-1, *et seq*

602. Anthem's acts and practices are unfair or unconscionable because Anthem's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with Anthem. Further, Anthem took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with

Anthem and consumers' inability to protect themselves due to the asymmetry of information concerning Anthem's data security practices.

603. Anthem's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Anthem's data security measures and ability to protect the confidentiality of consumers' PII and PHI.

604. Anthem's acts and practices, including its material omissions, were likely to, and did in fact, deceive and mislead members of the public, including consumers acting reasonably under the circumstances, to their detriment.

605. Anthem intended to mislead Plaintiff and Indiana Subclass Members and induce them to rely on its misrepresentations and omissions.

606. Anthem had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in its possession. This duty arose because members of the public, including Plaintiff and the Indiana Subclass Members, bestowed trust and confidence in Anthem to keep their PII and PHI secure. Anthem's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

607. Had Anthem disclosed to Plaintiff and the Indiana Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Anthem 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. Anthem was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and the Indiana Subclass Members. Anthem accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff

and the Indiana Subclass Members acted reasonably in relying on Anthem's misrepresentations and omissions, the truth of which they could not have discovered.

608. Anthem acted intentionally, knowingly, and maliciously to violate the IDCSA, and recklessly disregarded Plaintiff's and Indiana Subclass Members' rights. Anthem's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

609. Anthem's violations present a continuing risk to Plaintiff and the Indiana Subclass Members as well as to the general public.

610. As a direct and proximate result of Anthem's unfair, unconscionable, and deceptive practices, Plaintiff and the Indiana Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiff and Indiana Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) 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; (7) the continued risk to their PII and PHI, which remain in Anthem's possession and is subject to further unauthorized disclosures so long as Anthem fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data

security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

611. Plaintiff and the Indiana Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $500 for each non-willful violation; the greater or treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

CLAIMS ON BEHALF OF THE KANSAS SUBCLASS

COUNT XVI
KANSAS CONSUMER PROTECTION ACT
K.S.A. §§50-623, *et seq*.
(On Behalf of Plaintiff Tetreault and the Kansas Subclass and Against Aetna)

612. Plaintiff Tetreault (Plaintiff" for purposes of this Count), individually and on behalf of the Kansas Subclass Members, repeats and re-alleges all preceding allegations in paragraphs 1 through 385 as if fully set forth herein.

613. Plaintiff and Kansas Subclass Members are "consumers" as defined by K.S.A. §§50-624(b).

614. The acts and practices described herein are "consumer transactions," as defined by K.S.A. §50-624(c).

615. Defendant is a "supplier" as defined by K.S.A. §50-624(l).

616. Defendant advertised, offered, or sold goods or services in Kansas and engaged in trade or commerce directly or indirectly affecting the people of Kansas.

617. The Kansas Consumer Protection Act ("KCPA") is construed liberally to promote, among other things, policies to protect consumers from suppliers who commit deceptive and unconscionable practices. K.S.A. §50-623(b).

618. Aetna engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce in violation of K.S.A. §50-626.

619. Aetna's deceptive acts and practices include:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Kansas Subclass Member's PII and PHI;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Kansas Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Kansas' data breach notification statute, K.S.A. §50-7a02(a).

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Kansas Subclass Members' PII and PHI, including failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Kansas Subclass Members' PII and PHI; and

d. 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 Kansas Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Kansas' data breach notification statute, K.S.A. §50-7a02(a).

620. Aetna's unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Kansas Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiffs' and Kansas Subclass Members' PII and

PHI in exchange with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiff's and Kansas Subclass Members' PII and PHI;

b. Disclosing Plaintiffs' and Kansas Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law, statutory duties pertaining to the security and privacy of Plaintiff's and Kansas Subclass Members' PII and PHI, including duties imposed by the FTC ACT and HIPPA; and

d. Failing to comply with the duties imposed by Kansas' data breach notification statute, K.S.A§50-7a02(a) and disclose the Data Breach to Plaintiff and the Kansas Subclass in a timely and accurate manner.

621. Aetna's conduct constitutes unfair methods of competition or unfair or unconscionable practices within the meaning of KCPA because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Kansas Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiffs and the Kansas Subclass Members are not outweighed by any countervailing benefit to consumers or competition. And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiff's and Kansas Subclass Members' PII and PHI, there is no way Plaintiffs and the Kansas Subclass Members could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security, Aetna created an asymmetry of information between it

and consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

622. Aetna's conduct constitutes unfair practices within the meaning of KCPA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA as well as the Kansas data breach notification statute (K.S.A. §50-7a02(a)).

623. Aetna's acts and practices are unfair or unconscionable because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transaction with Aetna. Further, Aetna took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Aetna and consumers inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

624. Aetna acted intentionally, knowingly, and maliciously to violate the KCPA, and recklessly disregarded Plaintiff and the Kansas Subclass Members' rights.

625. As a direct and proximate result of Aetna's deceptive trade practices, Plaintiff and the Kansas Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and the monetary and non-monetary damages. Specifically, Plaintiff and Kansas Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1 actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) 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, efforts spent researching how to prevent, detect, consent, and recovery from identity theft; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized discloser so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

626. Plaintiff and the Kansas Subclass Members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A §§50-634 and 50-636; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE KENTUCKY SUBCLASS

COUNT XVII
KENTUCKY CONSUMER PROTECTION ACT
Ky. Rev. Stat. §§367.110, *et seq.*
(On Behalf of Plaintiff Marshall and the Kentucky Subclass and Against Elevance)

627. Plaintiff Marshall ("Plaintiff" for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeats all preceding allegations in paragraphs 1 through 385 as if fully set forth herein.

628. Elevance, Plaintiff, and each member of the Kentucky Subclass are "persons" as defined by Ky. Rev. Stat. §§367.110(1).

629. Elevance engaged in "trade" or "commerce" as defined by Ky. Rev. Stat. §§367.110(2).

630. Elevance engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Ky. Rev. Stat. §§367.170.

631. Elevance's deceptive acts and practices include:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Kentucky Subclass Members' PII and PHI;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Kentucky Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Ky. Rev. Stat. §§365.732, *et seq.*

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Kentucky Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Kentucky Subclass Members' PII and PHI; and

d. 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 Kentucky Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Ky. Rev. Stat. §§365.732, *et seq.*

632. Aetna's unfair or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Kentucky Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiff's and Kentucky Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its

vendors and business associates reasonably and adequately secured Plaintiff's and Kentucky Subclass Members' PII and PHI;

b. Disclosing Plaintiff's and Kentucky Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Kentucky Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA; and

d. Failing to comply with the duties imposed by Ky. Rev. Stat. §§365.732, *et seq*. and disclose the Data Breach to Plaintiff and the Kentucky Subclass Members in a timely and accurate manner.

633. Elevance's conduct constitutes unfair methods of competition or unfair or unconscionable practices within the meaning of the Kentucky Consumer Protection Act because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Kentucky Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiff and the Kentucky Subclass Members are not outweighed by any countervailing benefits to consumers or competition. And, because Elevance is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiff's and Kentucky Subclass Members' PII and PHI, there is no way Plaintiff and the Kentucky Subclass Members could have known about Elevance's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security, Elevance created an asymmetry of information between it and consumers that precluded

consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Elevance's legitimate business interests.

634. Elevance's conduct constitutes unfair practices within the meaning of Kentucky's Consumer Protection Act because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA as well as Ky. Rev. Stat. §§365.732, *et seq*.

635. Elevance's acts and practices are unfair or unconscionable because Elevance's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with Elevance. Further, Elevance took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Elevance and consumers' inability to protect themselves due to the asymmetry of information concerning Elevance's data security practices.

636. Elevance's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Elevance's data security measures and ability to protect the confidentiality of consumers' PII and PHI.

637. Elevance's acts and practices, including its material omissions, were likely to, and did in fact, deceive and mislead members of the public, including consumers acting reasonably under the circumstances, to their detriment.

638. Elevance intended to mislead Plaintiff and Kentucky Subclass Members and induce them to rely on its misrepresentations and omissions.

639. Elevance had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in its possession. This duty arose because members of the public, including Plaintiff and the Kentucky Subclass Members, bestowed trust and confidence in Elevance to keep their PII and PHI secure. Elevance's duty to disclose also

arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

640. Had Elevance disclosed to Plaintiff and the Kentucky Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Elevance 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. Elevance was trusted with sensitive and valuable PII and PHI regarding hundreds of thousands of consumers, including Plaintiff and the Kentucky Subclass Members. Elevance accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Kentucky Subclass Members acted reasonably in relying on Elevance's misrepresentations and omissions, the truth of which they could not have discovered.

641. Elevance's violations present a continuing risk to Plaintiff and the Kentucky Subclass Members as well as to the general public.

642. As a direct and proximate result of Elevance's unfair, unconscionable, and deceptive practices, Plaintiff and the Kentucky Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiff and Kentucky Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) 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; (7) the continued risk to their PII and PHI, which remain in Elevance's possession and is subject to further unauthorized disclosures so long as Elevance fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

643. Plaintiff and the Kentucky Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, restitution or other equitable relief, injunctive relief, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE MICHIGAN SUBCLASS

COUNT XVIII
MICHIGAN CONSUMER PROTECTION ACT
Mich. Comp. Laws Ann. §§445.903, et seq.
(On Behalf of Plaintiff Banks and the Michigan Subclass and Against Aetna)

644. Plaintiff Banks ("Plaintiff" for purposes of this Count), individually and on behalf of the Michigan Subclass Members, repeats and re-alleges all preceding allegations in paragraphs 1 through 385 as if fully set forth herein.

645. Aetna, Plaintiff, and each member of the Michigan Subclass are "persons" as defined by Mich. Comp. Laws Ann. §445.903(d).

646. Aetna advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. §445.903(g).

647. Aetna engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. §445.903(1),

648. Aetna's deceptive acts and practices include:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Michigan Subclass Members' PII and PHI;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Michigan Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Mich. Comp. Laws Ann. §§445.72, *et seq*.;

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Michigan Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Michigan Subclass Members' PII and PHI; and

d. 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 Michigan Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Mich. Comp. Laws Ann. §§445.72, *et seq*.

649. Aetna's unfair or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Michigan Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiff's and Michigan Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its

vendors and business associates reasonably and adequately secured Plaintiff's and Michigan Subclass Members' PII and PHI;

b. Disclosing Plaintiff's and Michigan Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Michigan Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA; and

d. Failing to comply with the duties imposed by Mich. Comp. Laws Ann. §§445.72, *et seq*. and disclose the Data Breach to Plaintiff and the Michigan Subclass Members in a timely and accurate manner.

650. Aetna's conduct constitutes unfair methods of competition or unfair or unconscionable practices within the meaning of the Michigan Consumer Protection Act ("Michigan CPA") because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Michigan Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiff and the Michigan Subclass Members are not outweighed by any countervailing benefits to consumers or competition. And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiff's and Michigan Subclass Members' PII and PHI, there is no way Plaintiff and the Michigan Subclass Members could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security, Aetna created an asymmetry of information between it and

consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

651. Aetna's conduct constitutes unfair practices within the meaning of Michigan CPA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA as well as Mich. Comp. Laws Ann. §§445.72, *et seq*.

652. Aetna's acts and practices are unfair or unconscionable because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with Aetna. Further, Aetna took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Aetna and consumers' inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

653. Aetna's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security measures and ability to protect the confidentiality of consumers' PII and PHI.

654. Aetna's acts and practices, including its material omissions, were likely to, and did in fact, deceive and mislead members of the public, including consumers acting reasonably under the circumstances, to their detriment.

655. Aetna intended to mislead Plaintiff and Michigan Subclass Members and induce them to rely on its misrepresentations and omissions.

656. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in its possession. This duty arose because members of the public, including Plaintiff and the Michigan Subclass Members, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from

its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

657. Had Aetna disclosed to Plaintiff and the Michigan Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna 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. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and the Michigan Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Michigan Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

658. Aetna acted intentionally, knowingly, and maliciously to violate the Michigan CPA, and recklessly disregarded Plaintiff's and Michigan Subclass Members' rights. Aetna's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

659. Aetna's violations present a continuing risk to Plaintiff and the Michigan Subclass Members as well as to the general public.

660. As a direct and proximate result of Aetna's unfair, unconscionable, and deceptive practices, Plaintiff and the Michigan Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiff and Michigan Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially

increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) 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; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

661. Plaintiff and the Michigan Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, injunctive relief, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE NEVADA SUBCLASS

COUNT XIX
NEVADA DECEPTIVE TRADE PRACTICES ACT
Nev. Rev. Stat. §§598.0901, et seq.
(On Behalf of Plaintiff Keep and the Nevada Subclass and Against Aetna)

662. Plaintiff Keep ("Plaintiff" for purposes of this Count), individually and on behalf of the Nevada Subclass, repeats and re-alleges all preceding allegations in paragraphs 1 through 385 as if fully set forth herein.

663. The Nevada Deceptive Trade Practices Act ("NDTPA") prohibits deceptive or unconscionable trade practices in the course of business.

664. In the course of its business, Aetna operating in Nevada engaged in deceptive or unconscionable acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of health insurance and health benefits services in violation of Nev. Rev. Stat. §598.0901, *et seq*., including Nev. Rev. Stat. §§598.915(5), (7), (9), (15) and Nev. Rev. Stat. §§598.923(1)(b), (c), (e), and Nev. Rev. Stat. §§603A.010, *et seq*.

665. Aetna's deceptive or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Nevada Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiff's and Nevada Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiff's and Nevada Subclass Members' PII and PHI;

b. Disclosing Plaintiff's and Nevada Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the Nevada Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA;

d. Failing to comply with the duties imposed by Nev. Rev. Stat. §§603A.010, *et seq*. and disclose the Data Breach to Plaintiff and the Nevada Subclass Members in a timely and accurate manner;

e. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and the Nevada Subclass Members' PII and PHI;

f. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the Nevada Subclass' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Nev. Rev. Stat. §§603A.010, *et seq*.;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and the Nevada Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Nevada Subclass Members' PII and PHI; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the Nevada Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Nev. Rev. Stat. §§ 603A.010, *et seq*.

666. Aetna's conduct constitutes unconscionable practices within the meaning of NDTPA because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates

reasonably or adequately secured Plaintiff's and Nevada Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiff and the Nevada Subclass are not outweighed by any countervailing benefits to consumers or competition. And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiff's and Nevada Subclass Members' PII and PHI, there is no way Plaintiff and the Nevada Subclass Members could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security measures, Aetna created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

667. Aetna's acts and practices are unconscionable because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with Aetna. Further, Aetna took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Aetna and consumers' inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

668. Aetna's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security and ability to protect the confidentiality of consumers' PII and PHI.

669. Aetna intended to mislead Plaintiff and the Nevada Subclass and induce them to rely on its misrepresentations and omissions.

670. In the course of its business, Aetna engaged in activities with a tendency or capacity to deceive.

671. Aetna acted intentionally, knowingly, and maliciously to violate the NDTPA, and recklessly disregarded Plaintiff and the Nevada Subclass Members' rights.

672. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in their possession. This duty arose because members of the public, including Plaintiff and the Nevada Subclass, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

673. Had Aetna disclosed to Plaintiff and the Nevada Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna 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. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and the Nevada Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Nevada Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

674. Aetna's violations present a continuing risk to Plaintiff and the Nevada Subclass as well as to the general public.

675. As a direct and proximate result of Aetna's deceptive and unconscionable trade practices, Plaintiff and the Nevada Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages.

Specifically, Plaintiff and Nevada Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) 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; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

676. Plaintiff and the Nevada Subclass Members seek all monetary and non-monetary relief allowed by Nev. Rev. Stat. §41.600 and any other legal authority, including but not limited to damages, punitive damages, equitable relief, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

COUNT XX
NEW YORK GENERAL BUSINESS LAW
N.Y. Gen. Bus. Law §§349, et seq.
(On Behalf of Plaintiffs Rougeau, N. Venezia, V. Venezia and the New York Subclass and Against Aetna)

677. Plaintiffs Rougeau, N. Venezia, and V. Venezia ("Plaintiffs" for purposes of this Count) individually and on behalf of the New York Subclass, repeat and re-allege all preceding allegations in paragraphs 1 through 385 as if fully set forth herein.

678. New York General Business Law §349 ("GBL §349") prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service" in New York. Plaintiffs and the New York Subclass are consumers that reside in New York who purchased insurance and health benefits services from Aetna.

679. Aetna engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of GBL §349.

680. Aetna's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and New York Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiff's and New York Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiffs' and New York Subclass Members' PII and PHI;

b. Disclosing Plaintiffs' and New York Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and the New York Subclass' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as N.Y. Gen. Bus. Law §899-aa;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs and the New York Subclass Members' PII and PHI;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the New York Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as N.Y. Gen. Bus. Law §899-aa;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and the New York Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiffs' and New York Subclass Members' PII and PHI; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the New York Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as N.Y. Gen. Bus. Law §899-aa.

681. Aetna's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security and ability to protect the confidentiality of consumers' PII and PHI.

682. Aetna intended to mislead Plaintiffs and the New York Subclass Members and induce them to rely on its misrepresentations and omissions.

683. In the course of its business, Aetna engaged in activities with a tendency or capacity to deceive.

684. Aetna acted intentionally, knowingly, and maliciously to violate GBL §349 and recklessly disregarded Plaintiffs and the New York Subclass Members' rights.

685. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in its possession. This duty arose because members of the public, including Plaintiffs and the New York Subclass Members, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

686. Had Aetna disclosed to Plaintiffs and the New York Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna 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. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiffs and the New York Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and the New York Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

687. Aetna's deceptive and unlawful acts and practices complained of herein affected consumers and the public interest and consumers at large, including at least hundreds of New

Yorkers affected by the Data Breach. Aetna's deceptive acts and practices were likely to and did in fact deceive the public at large and reasonable consumers, including Plaintiffs and the New York Subclass Members, regarding Aetna's data security measures and supervision of its vendors' and business associates' data security measures.

688. Aetna's violations present a continuing risk to Plaintiffs and the New York Subclass Members as well as to the general public.

689. Thus, Plaintiffs bring this action on behalf of themselves and the New York Subclass Members for the public benefit in order to promote the public interests in the provision of truthful, fair information that enables consumers and the public at large to make informed decisions related to the security of their PII and PHI, and to protect the public from Aetna's unlawful acts and practices.

690. As a direct and proximate result of Aetna's deceptive and unlawful acts and practices, Plaintiffs and the New York Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiffs and New York Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) 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; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

691. Plaintiffs and the New York Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

CLAIMS ON BEHALF OF THE NORTH CAROLINA SUBCLASS

COUNT XXI
NORTH CAROLINA IDENTITY THEFT PROTECTION ACT, N.C. Gen. Stat. §75-1.1, *et seq.*
(On Behalf of Plaintiff Eddie and the North Carolina Subclass and Against Aetna)

692. Plaintiff Eddie ("Plaintiff" for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and re-alleges all preceding allegations in paragraphs 1-385 as if fully set forth herein.

693. Pursuant to N.C. Gen. Stat. §75-1.1(a), "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful."

694. Aetna engaged in "commerce" as defined by N.C. Gen. Stat. §75-1.1(b).

695. Aetna engaged in deceptive acts or practices in the conduct of its business activities, in violation of N.C. Gen. Stat. §75-1.1, *et seq*.

696. Aetna's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and North Carolina Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiff's and North Carolina Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiffs' and North Carolina Subclass Members' PII and PHI;

b. Disclosing Plaintiffs' and North Carolina Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and the North Carolina Subclass' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as N.C. Gen. Stat. §75-65, *et seq*;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs and the North Carolina Subclass Members' PII and PHI;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the North Carolina Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as N.C. Gen. Stat. §75-65, *et seq*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and the North Carolina Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors

and business associates reasonably or adequately secured Plaintiffs' and New York Subclass Members' PII and PHI; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the North Carolina Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as N.C. Gen. Stat. §75-65, *et seq*.

697. Aetna's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security and ability to protect the confidentiality of consumers' PII and PHI.

698. Aetna intended to mislead Plaintiffs and the North Carolina Subclass Members and induce them to rely on its misrepresentations and omissions.

699. In the course of its business, Aetna engaged in activities with a tendency or capacity to deceive.

700. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in its possession. This duty arose because members of the public, including Plaintiffs and the North Carolina Subclass Members, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

701. Had Aetna disclosed to Plaintiffs and the North Carolina Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna 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. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiffs and the North Carolina Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and the North Carolina Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

702. Aetna's deceptive and unlawful acts and practices complained of herein affected at least hundreds of North Carolina consumers affected by the Data Breach. Aetna's deceptive acts and practices were likely to and did in fact deceive the public at large and reasonable consumers, including Plaintiffs and the North Carolina Subclass Members, regarding Aetna's data security measures and supervision of its vendors' and business associates' data security measures.

703. Aetna's violations present a continuing risk to Plaintiffs and the North Carolina Subclass Members as well as to the general public.

704. Thus, Plaintiffs bring this action on behalf of themselves and the North Carolina Subclass Members for the public benefit in order to promote the public interests in the provision of truthful, fair information that enables consumers and the public at large to make informed decisions related to the security of their PII and PHI, and to protect the public from Aetna's unlawful acts and practices.

705. As a direct and proximate result of Aetna's deceptive and unlawful acts and practices, Plaintiffs and the North Carolina Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiffs and North Carolina Subclass Members have suffered and will continue to

suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) 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; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

706. Plaintiff and North Carolina Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NORTH DAKOTA SUBCLASS

COUNT XXII
NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT
N.D. Cent. Code §§51-15-01, *et seq*.
(On Behalf of Plaintiff Ronne and the North Dakota Subclass and Against Aetna)

707. Plaintiff Ronne ("Plaintiff" for purposes of this Count), individually and on behalf of the North Dakota Subclass, repeats and re-alleges all preceding allegations in paragraphs 1 thought 385 as if fully set forth herein.

708. Aetna, Plaintiff Ronne, and each member of the North Dakota Subclass is a "person" as defined by N.D. Cent. Code §51-15-01(4).

709. Aetna sells and advertises "merchandise," as defined by N.D. Cent. Code §51-15-01(3) and (5) in the form of insurance and health benefits services.

710. Aetna advertised, offered, or sold goods or services in North Dakota and engaged in trade or commerce directly or indirectly affecting the people of North Dakota.

711. Aetna engaged in deceptive, false, fraudulent, misrepresentative, unconscionable, and substantially injurious acts and practices in connection with the sale and advertisement of merchandise, in violation of N.D. Cent. Code §51-15-01.

712. Aetna's unlawful acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and North Dakota Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiff's and North Dakota Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiff's and North Dakota Subclass Members' PII and PHI;

b. Disclosing Plaintiff's and North Dakota Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the PII and PHI, including duties imposed by the FTC Act and HIPAA as well as North Dakota's prohibited practices in insurance business act, N.D. Cent. Code §§26.1-04-01, *et seq.*, and North Dakota's data breach notification statute, N.D. Cent. Code §§ 51-30-02, *et seq*.;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and the North Dakota Subclass Members' PII and PHI;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and the North Dakota Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as North Dakota's prohibited practices in insurance business act, N.D. Cent. Code §§26.1-04-01, *et seq.*, and North Dakota's data breach notification statute, N.D. Cent. Code §§51-30-02, *et seq*.;

f. Engaged in unfair methods of competition or unfair or deceptive acts or practices in the business of insurance, in violation of N.D. Cent. Code §26.1-04-03(1) and N.D. Cent. Code §26.1-04-03(2);

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and the North Dakota Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors

and business associates reasonably or adequately secured Plaintiff's and North Dakota Subclass Members' PII and PHI; and

h. 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 the North Dakota Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as North Dakota's prohibited practices in insurance business act, N.D. Cent. Code §§ 26.1-04-01, *et seq.*, and North Dakota's data breach notification statute, N.D. Cent. Code §§51-30-02, *et seq*.

713. Aetna's conduct constitutes unfair methods of competition or unfair or unconscionable practices within the meaning of the North Dakota Unlawful Sales or Advertising Act ("North Dakota USAA") because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and North Dakota Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiff and the North Dakota Subclass Members are not outweighed by any countervailing benefits to consumers or competition. And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiff's and North Dakota Subclass Members' PII and PHI, there is no way Plaintiff and the North Dakota Subclass Members could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security, Aetna created an asymmetry of information

between it and consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

714. Aetna's conduct constitutes unfair practices within the meaning of North Dakota USAA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA as well as North Dakota's prohibited practices in insurance business act, N.D. Cent. Code §§26.1-04-01, *et seq.*, and North Dakota's data breach notification statute, N.D. Cent. Code §§51-30-02, *et seq*.

715. Aetna's acts and practices are unfair or unconscionable because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with Aetna. Further, Aetna took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Aetna and consumers' inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

716. Aetna's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security and ability to protect the confidentiality of consumers' PII and PHI.

717. Aetna intended to mislead Plaintiff and the North Dakota Subclass Members and induce them to rely on its misrepresentations and omissions.

718. In the course of its business, Aetna engaged in activities with a tendency or capacity to deceive.

719. Aetna acted intentionally, knowingly, and maliciously to violate North Dakota's USAA, and recklessly disregarded Plaintiff and the North Dakota Subclass Members' rights.

720. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in its possession. This duty arose because members of the public, including Plaintiff and the North Dakota Subclass Members, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

721. Had Aetna disclosed to Plaintiff and the North Dakota Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna 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. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and the North Dakota Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the North Dakota Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

722. Aetna's violations present a continuing risk to Plaintiff and the North Dakota Subclass Members as well as to the general public.

723. As a direct and proximate result of Aetna's deceptive, unconscionable, and substantially injurious practices, Plaintiff and the North Dakota Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiff and North Dakota Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2)

a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) 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; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

724. Plaintiff and the North Dakota Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, restitution, treble damages, civil penalties, and attorneys' fees, costs, and disbursements.

CLAIMS ON BEHALF OF THE OHIO SUBCLASS

COUNT XXIII
OHIO CONSUMER SALES PRACTICES ACT
Ohio Rev. Code §§1345.01, *et seq*.
(On Behalf of Plaintiffs D. Vogel, J. Vogel and the Ohio Subclass and Against Aetna)

725. Plaintiffs D. Vogel and J. Vogel ("Plaintiffs" for purposes of this Count), individually and on behalf of the Ohio Subclass, repeat and re-allege all preceding allegations in paragraphs 1 through 385 as if fully set forth herein.

726. Aetna, Plaintiffs, and each member of the Ohio Subclass are "persons," as defined by Ohio Rev. Code §1345.01(B).

727. Aetna was a "supplier" engaged in "consumer transactions," as defined by Ohio Rev. Code §§1345.01(A) & (C).

728. Aetna advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

729. Aetna engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code §1345.02, including:

a. Representing that the subject of a transaction had approval, performance characteristics, uses, and benefits that it did not have; and

b. Representing that the subjects of a transaction were of a particular standard or quality when they were not.

730. Aetna engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code §1345.03, including:

a. Knowingly taking advantage of the inability of Plaintiffs and Ohio Subclass Members to reasonably protect their interests because of their ignorance of the issues discussed herein;

b. Knowing at the time the consumer transaction was entered into of the inability of the consumer to receive a substantial benefit from the subject of the consumer transaction;

c. Requiring the consumer to enter into a consumer transaction on terms the supplier knew were substantially one-sided in favor of the supplier;

d. Knowingly making a misleading statement of opinion on which the consumer was likely to rely to the consumer's detriment.

731. Aetna's deceptive acts and practices include:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Ohio Subclass Members' PII and PHI;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Ohio Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Ohio's data breach notification statute, Ohio Rev. Code §1349.19;

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Ohio Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiffs' and Ohio Subclass Members' PII and PHI; and

d. 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 Plaintiffs' and Ohio Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Ohio's data breach notification statute, Ohio Rev. Code §1349.19.

732. Aetna's unfair or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Ohio Subclass Members' PII and PHI,

including by failing to properly secure and encrypt Plaintiffs' and Ohio Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiffs' and Ohio Subclass Members' PII and PHI;

b. Disclosing Plaintiffs' and Ohio Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so; and

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Ohio Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Ohio's data breach notification statute, Ohio Rev. Code §1349.19.

733. Aetna's conduct constitutes unfair methods of competition or unfair or unconscionable practices within the meaning of the Ohio Consumer Sales Practices Act ("OCSPA") because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiffs' and Ohio Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiffs and the Ohio Subclass Members are not outweighed by any countervailing benefits to consumers or competition. And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiffs' and Ohio Subclass Members' PII and PHI, there is no way Plaintiffs and the Ohio Subclass Members could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data

security, Aetna created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

734. Aetna's conduct constitutes unfair practices within the meaning of OCSPA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA as well as Ohio's data breach notification statute, Ohio Rev. Code §1349.19.

735. Aetna's acts and practices are unfair or unconscionable because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with Aetna. Further, Aetna took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Aetna and consumers' inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

736. Aetna's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security measures and ability to protect the confidentiality of consumers' PII and PHI.

737. Aetna's acts and practices, including its material omissions, were likely to, and did in fact, deceive and mislead members of the public, including consumers acting reasonably under the circumstances, to their detriment.

738. Aetna intended to mislead Plaintiffs and Ohio Subclass Members and induce them to rely on its misrepresentations and omissions.

739. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in its possession. This duty arose because members of the public, including Plaintiffs and the Ohio Subclass Members, bestowed trust and

confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

740. Had Aetna disclosed to Plaintiffs and the Ohio Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna 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. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiffs and the Ohio Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and the Ohio Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

741. Aetna acted intentionally, knowingly, and maliciously to violate the OCSPA and recklessly disregarded Plaintiffs' and Ohio Subclass Members' rights.

742. Aetna's violations present a continuing risk to Plaintiffs and the Ohio Subclass Members as well as to the general public.

743. As a direct and proximate result of Aetna's unfair, deceptive, and unconscionable acts and practices, Plaintiffs and the Ohio Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiffs and Ohio Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and

PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) 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; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the goods and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

744. Plaintiffs and the Ohio Subclass Members seek all monetary and non-monetary relief allowed by law, including declaratory and injunctive relief, the greater of actual and treble damages or statutory damages, attorneys' fees and costs, and any other appropriate relief.

CLAIMS ON BEHALF OF THE OKLAHOMA SUBCLASS

COUNT XXIV
OKLAHOMA CONSUMER PROTECTION ACT
15 Okla. Stat. §§751, et seq.
(On Behalf of Plaintiffs Brewer, Carter and the Oklahoma Subclass and Against Aetna)

745. Plaintiffs Brewer and Carter ("Plaintiffs" for purposes of this Count), individually and on behalf of the Oklahoma Subclass, repeat and re-allege all preceding allegations in paragraphs 1 through 385 as if fully set forth herein.

746. Plaintiffs and the Oklahoma Subclass Members purchased "merchandise," as meant by 15 Okla. Stat. §752(7), in the form of insurance and health benefits services.

747. Plaintiffs and the Oklahoma Subclass Members' purchases of insurance and health benefits services from Aetna constituted "consumer transactions" as meant by 15 Okla. Stat. §752(2).

748. Aetna is a "person" as defined by 15 Okla. Stat. §752(1).

749. Aetna, in the course of its business, engaged in unlawful practices in violation of 15 Okla. Stat. §753, including the following:

a. Making false or misleading representations, knowingly or with reason to know, as to the characteristics, uses, and benefits of the subjects of its consumer transactions;

b. Representing, knowingly or with reason to know, that the subjects of its consumer transactions were of a particular standard when they were of another;

c. Advertising, knowingly or with reason to know, the subjects of its consumer transactions with intent not to sell as advertised;

d. Committing deceptive trade practices that deceived or could reasonably be expected to deceive or mislead a person to the detriment of that person as defined by §752(13); and

e. Committing unfair trade practices that offend established public policy and was immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers as defined by §752(14).

750. Aetna's deceptive acts and practices include:

f. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Oklahoma Subclass Members' PII and PHI;

g. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Oklahoma Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Oklahoma's data breach notification statute, 24 Okla. Stat. §161 *et seq.*;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Oklahoma Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiffs' and Oklahoma Subclass Members' PII and PHI; and

i. 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 Plaintiffs' and Oklahoma Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as Oklahoma's data breach notification statute, 24 Okla. Stat. §161 *et seq*.

751. Aetna's unfair acts and practices include:

j. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Oklahoma Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiffs' and Oklahoma Subclass Members' PII and PHI exchanged with NationsBenefits and failing to reasonably ensure its vendors and business associates reasonably and adequately secured Plaintiffs' and Oklahoma Subclass Members' PII and PHI;

k. Disclosing Plaintiffs' and Oklahoma Subclass Members' PII and PHI to NationsBenefits without a legitimate business reason to do so;

l. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Oklahoma Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA; and

m. Failing to comply with the duties imposed by 24 Okla. Stat. §161, *et seq*. and disclose the Data Breach to Plaintiffs and the Oklahoma Subclass Members in a timely and accurate manner.

752. Aetna's conduct constitutes unfair methods of competition and unfair practices within the meaning of the Oklahoma Consumer Protection Act ("Oklahoma CPA") because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Aetna cut corners and minimized costs by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiffs' and Oklahoma Subclass Members' PII and PHI. Further, the injuries suffered by Plaintiffs and the Oklahoma Subclass Members are not outweighed by any countervailing benefits to consumers or competition. And, because Aetna is solely responsible for reasonably ensuring its vendors and business associates reasonably or adequately secured Plaintiffs' and Oklahoma Subclass Members' PII and PHI, there is no way Plaintiffs and the Oklahoma Subclass could have known about Aetna's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security, Aetna created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further Aetna's legitimate business interests.

753. Aetna's conduct constitutes unfair practices within the meaning of Oklahoma CPA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA as well as Oklahoma's data breach notification statute, 24 Okla. Stat. §161, *et seq*.

754. Aetna's acts and practices are unfair because Aetna's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with Aetna. Further, Aetna took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with Aetna and consumers' inability to protect themselves due to the asymmetry of information concerning Aetna's data security practices.

755. Aetna's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Aetna's data security measures and ability to protect the confidentiality of consumers' PII and PHI.

756. Aetna's acts and practices, including its material omissions, were likely to, and did in fact, deceive and mislead members of the public, including consumers acting reasonably under the circumstances, to their detriment.

757. Aetna intended to mislead Plaintiffs and Oklahoma Subclass Members and induce them to rely on its misrepresentations and omissions.

758. Aetna had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in its possession. This duty arose because members of the public, including Plaintiffs and the Oklahoma Subclass Members, bestowed trust and confidence in Aetna to keep their PII and PHI secure. Aetna's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

759. Had Aetna disclosed to Plaintiffs and the Oklahoma Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, Aetna 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. Aetna was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiffs and the Oklahoma Subclass Members. Aetna accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and the Oklahoma Subclass Members acted reasonably in relying on Aetna's misrepresentations and omissions, the truth of which they could not have discovered.

760. Aetna acted intentionally, knowingly, and maliciously to violate Oklahoma CPA, and recklessly disregarded Plaintiffs' and Oklahoma Subclass Members' rights.

761. Aetna's violations present a continuing risk to Plaintiffs and the Oklahoma Subclass Members as well as to the general public.

762. As a direct and proximate result of Aetna's unlawful practices, Plaintiffs and the Oklahoma Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII and PHI, and monetary and non-monetary damages. Specifically, Plaintiffs and Oklahoma Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) actual identity theft; (2) a substantially increased and imminent risk of identity theft; (3) the loss of the opportunity to determine how their PII and PHI is used; (4) the compromise, publication, and/or theft of their PII and PHI; (5) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (6) 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; (7) the continued risk to their PII and PHI, which remain in Aetna's possession and is subject to further unauthorized disclosures so long as Aetna fails to undertake appropriate and adequate measures to protect the PII and PHI in its possession; (8) overpayment for the good and services that were received without adequate data security; (9) lost value of their PII and PHI; and (10) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

763. Plaintiffs and the Oklahoma Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, civil penalties, equitable relief, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, request the following relief:

A. An Order certifying this action as a class action and appointing Plaintiffs as Class representatives and the undersigned as Class Counsel;

B. A declaration that Defendants breached their duties to Plaintiffs and Class Members;

C. A mandatory injunction directing Defendants to adequately safeguard the Personal Information of Plaintiffs and the Classes hereinafter by implementing improved security and vendor risk management procedures and measures;

D. A mandatory injunction requiring that Defendants provide notice to each member of the Classes relating to the full nature and extent of the Data Breach and the disclosure of Personal Information to unauthorized persons;

E. An injunction on Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen Personal Information;

F. An award of damages, including actual, nominal, consequential damages, statutory, and/or punitive, as allowed by law in an amount to be determined;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. For all other Orders, findings, and determinations identified and sought in this Complaint; and

I. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury for all issues so triable as of right.

Dated: April 18, 2024

Respectfully Submitted,

By: *Jeff Ostrow*

Jeff Ostrow FBN 121452
KOPELOWITZ OSTROW
FERGUSON WEISELBERG GILBERT
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: (954) 332-4200
ostrow@kolawyers.com

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
John Allen Yanchunis FBN 324681
201 N. Franklin St., 7th Floor
Tampa, FL 33602

Telephone: (813) 275-5272
jyanchunis@forthepeople.com

MDL Co-Lead Counsel for Plaintiffs

CARELLA, BYRNE, CECCHI, OLSTEIN, BRODY & AGNELLO, P.C.
James E. Cecchi (*pro hac vice*)
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973) 994-1700
jcecchi@carellabyrne.com

MDL Track Coordination and Settlement Counsel for Plaintiffs

ROBBINS GELLER RUDMAN & DOWD LLP
STUART A. DAVIDSON FBN 84824
225 N.E. Mizner Boulevard, Suite 720
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)
sdavidson@rgrdlaw.com

SILVER GOLUB & TEITELL LLP
IAN W. SLOSS (*pro hac vice*)
One Landmark Square
15th Floor
Stamford, CT 06901
Telephone: 203/325-4491
203/325-3769 (fax)
isloss@sgtlaw.com

MCSHANE & BRADY LLC
MAUREEN M. BRADY (*pro hac vice*)
1656 Washington Street, Suite 120
Kansas City, MO 64108
Tel: (816) 888-8010
Fax: (816) 332-6295
mbrady@mcshanebradylaw.com

SIRI & GLIMSTAD LLP
MASON A. BARNEY
745 Fifth Avenue, Suite 500
New York, NY 10151

Tel: (646) 357-1732
mbarney@sirillp.com

Plaintiffs' Track Three Leads

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing has been served via the CM/ECF system on all counsel of record on this 18th day of April, 2024.

/s/ Jeff Ostrow
Jeff Ostrow