IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

DAVID HARRELL, individually and on behalf of all others similarly situated, Plaintiff, v. WEBTPA EMPLOYER SERVICES, LLC; HARTFORD LIFE AND ACCIDENT INSURANCE COMPANY; ANTHEM BLUE CROSS LIFE AND HEALTH INSURANCE COMPANY; and ELEVANCE HEALTH, INC., Defendants.	Civil Action No.: 3:24-cv-01158-L Consolidated with Civil Actions Nos. 3:24-cv-01160; 3:24-cv-01164; 3:24-cv-01172; 3:24-cv-01174; 3:24-cv-01179; 3:24-cv-01180; 3:24-cv-01206; 3:24-cv-01210; 3:24-cv-01236; 3:24-cv-01242; 3:24-cv-01235; 3:24-cv-01264; 3:24-cv-01322; and 3:24-cv-01343 **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Tracy Bertocchini, Mark Ellak, Cory France, Chandra Chang, Conrad Heller, Sofia Bersineva, Heavenle Wood, Cynthia Austing, Belinda Gullette, Chanelle Zimmerman, Leonard Finkel, Michael Brown, and Kenneth Reagan (collectively "Plaintiffs"), individually and on behalf of all others similarly situated, bring this action against Defendants, WebTPA Employer Services, LLC ("WebTPA"); Hartford Life and Accident Insurance Company ("Hartford"); Anthem Blue Cross Life and Health Insurance Company ("Anthem BCBS"); and Elevance Health Inc. ("Elevance") (collectively, "Defendants"), alleging as follows, based upon personal knowledge and investigation of counsel.

I. INTRODUCTION

1. This class action arises from Defendants' failure to properly secure and safeguard Plaintiffs' and approximately 2,492,175 Class Members' sensitive personal health information ("PHI") and personal identifiable information ("PII") (PII and PHI collectively, "Private

Information"), which as a result, is now in criminal cyberthieves' possession.

2. Between March 6 and May 12, 2023, criminal hackers accessed WebTPA's network systems and stole Plaintiffs' and Class Members' Private Information stored therein, including their full names, contact information, dates of birth, Social Security numbers, and health insurance information (the "Data Breach"), causing Plaintiffs and Class Members widespread injuries and damages. The Data Breach is the direct result of Defendants' failure to implement even basic data security measures or oversight to reasonably protect Plaintiffs' and Class Members' Private Information in their custody and control.

3. Plaintiffs and Class Members are current and former insureds under insurance and benefit plans provided and/or serviced by Hartford, Anthem, and Elevance (collectively, "Insurer Defendants"). As a condition of obtaining insurance products and related services, Plaintiffs and Class Members were required to entrust their sensitive, non-public Private Information to Insurer Defendants and, through Insurer Defendants, to WebTPA.

4. WebTPA is a third-party vendor that provides custom health plans and contract administrative services to insurance and benefit company and employer group health plan clients across the United States, including Insurer Defendants. In this role to facilitate its services, WebTPA collected, used and maintained the Private Information of Insurer Defendants' customers—Plaintiffs and Class Members—in WebTPA's network systems.

5. Businesses that handle consumers' Private Information like Defendants owe the individuals to whom the information relates a duty to adopt reasonable measures to protect it from disclosure to unauthorized third parties, and to keep it safe and confidential. This duty arises under contract, statutory and common law, industry standards, representations made to Plaintiffs and Class Members, and because it is foreseeable that the exposure of Private Information to

unauthorized persons—and especially hackers with nefarious intentions—will harm the affected individuals, including but not limited to the invasion of their private health and financial matters.

6. Insurer Defendants separately had a duty to maintain the security of Plaintiffs' and Class Members' Private Information, and to ensure that their HIPAA business associate, WebTPA, had adequate, reasonable, and HIPAA-compliant data security to safeguard the Private Information Insurer Defendants furnished it.

7. Defendants breached their duties owed to Plaintiffs and Class Members by failing to safeguard the Private Information that Defendants collected and maintained, including by failing to implement industry standards for data security to protect against cyberattacks and by failing to reasonably supervise their vendor's cybersecurity practices, which allowed criminal hackers to access and steal millions of individuals' Private Information from Defendants' care.

8. According to WebTPA's May 8, 2024, notice to victims of the Data Breach ("Notice Letter"), on or about December 28, 2023, it "detected evidence of suspicious activity on the WebTPA network." WebTPA's ensuing investigation revealed that during the incident, in or around April 2023, an unauthorized actor accessed and obtained individuals' Private Information from WebTPA's network systems.

9. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendants, and thus, Defendants knew that failing to take reasonable steps to secure the Private Information left it in a dangerous condition.

10. Defendants failed to adequately protect Plaintiffs' and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive data or ensure the same from their vendor handling it. This unencrypted, unredacted Private Information was

compromised due to Defendants' negligent and/or careless acts and omissions and their utter failure to protect Plaintiffs' and Class Members' sensitive data.

11. Defendants breached their duties and obligations by failing, in one or more of the following ways: (a) to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (b) to design, implement, and maintain reasonable data retention policies; (c) to adequately train or oversee staff and service providers regarding data security; (d) failing to comply with industry-standard data security practices; (e) to warn Plaintiffs and Class Members of Defendants' inadequate data security practices; (f) to encrypt or adequately encrypt the Private Information; (g) to ensure their vendor handling PHI had HIPAA-compliant data security to protect it; (h) to recognize or detect that WebTPA's network had been compromised and accessed in a timely manner to mitigate the harm; (i) to utilize, or to ensure their vendor utilized, widely available software able to detect and prevent this type of attack; (j) and to otherwise secure the Private Information using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

12. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality and security of their Private Information. In providing their Private Information to Defendants, Plaintiffs and the Class Members reasonably expected these sophisticated business entities to keep their Private Information confidential and security maintained, to use this information for business purposes, and to disclose it only as authorized. Defendants failed to do so, resulting in the unauthorized disclosure of their Private Information in the Data Breach.

13. Hackers targeted and obtained Plaintiffs' and Class Members' Private Information from Defendants because of the data's value in exploiting and stealing Plaintiffs' and Class Members' identities. As a direct and proximate result of Defendants' inadequate data security and

breaches of their duties to handle Private Information with reasonable care, Plaintiffs' and Class Members' Private Information was accessed by cybercriminals and exposed to an untold number of unauthorized individuals. The present and continuing risk to Plaintiffs and Class Members as victims of the Data Breach will remain for their respective lifetimes.

14. The harm resulting from a cyberattack like this Data Breach manifests in numerous ways including identity theft and financial fraud, and the exposure of an individual's Private Information due to breach ensures that the individual will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of his or her life. Mitigating that risk, to the extent even possible, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take several additional prophylactic measures.

15. The risk of identity theft caused by this Data Breach is impending and has materialized, as there is evidence that the Plaintiffs' and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web.

16. To make matters worse, although Defendants confirmed the Data Breach's occurrence by March 25, 2024, they waited an additional six weeks before notifying Plaintiffs and Class Members—*over a year* after the Data Breach happened—that their Private Information had been compromised, diminishing Plaintiffs' and Class Members' ability to timely and thoroughly mitigate and address harms resulting from the Data Breach.

17. As a result of the Data Breach, Plaintiffs and Class Members, suffered concrete injuries in fact including, but not limited to (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) actual identity theft and

fraud; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their Private Information; (g) loss of privacy; (h) emotional distress including anxiety and stress in with dealing with the Data Breach; and (i) the continued risk to their sensitive Private Information, which remains in Defendants' possession and subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect the patient data they collect and maintain.

18. To recover for these harms, Plaintiffs, on behalf of themselves and the Class as defined herein, bring claims for negligence/negligence *per se*, breach of implied contract, breach of third-party beneficiary contract, violations of state consumer protection statutes, and unjust enrichment to address Defendants' inadequate safeguarding of Plaintiffs' and Class Members' Private Information in Defendants' custody and Defendants' failure to provide timely or adequate notice to Plaintiffs and Class Members that their information was compromised in the Data Breach.

19. Plaintiffs and Class Members seek compensatory, nominal, statutory, and punitive damages, declaratory judgment, and injunctive relief requiring Defendants to (a) disclose, expeditiously, the full nature of the Data Breach and the types of Private Information exposed; (b) implement improved data security practices to reasonably guard against future breaches of Private Information in Defendants' possession; and (c) provide, at Defendants' own expense, all impacted Data Breach victims with lifetime identity theft protection services.

II. THE PARTIES

Hartford Plaintiffs

20. Plaintiff Tracey Bertocchini is a citizen and resident of California.

21. Plaintiff Mark Ellak is a citizen and resident of California.

22. Plaintiff Cory France is a citizen and resident of Florida.

23. Plaintiff Chandra Chang is a citizen and resident of Georgia.

24. Plaintiff Conrad Heller is a citizen and resident of Georgia.

25. Plaintiff Sofia Bersineva is a citizen and resident of Illinois.

26. Plaintiff Leonard Finkel is a citizen and resident of New York.

27. Plaintiff Heavenle Wood is a citizen and resident of North Carolina.

28. Plaintiff Cynthia Austing is a citizen and resident of Ohio.

29. Plaintiff Belinda Gullette is a citizen and resident of Ohio.

30. Plaintiff Chanelle Zimmerman is a citizen and resident of Pennsylvania.

31. Plaintiffs Bertocchini, Ellak, France, Chang, Heller, Bersineva, Wood, Austing, Gullette, Zimmerman, and Finkel are hereinafter referred to collectively as "Hartford Plaintiffs."

32. At all relevant times, Hartford Plaintiffs received healthcare coverage and related services from Hartford. As a condition of and in exchange for their receipt of healthcare coverage and services, each Hartford Plaintiff was required to provide his or her Private Information to Hartford, and through Hartford, to WebTPA.

Anthem Plaintiffs

33. Plaintiff Michael Brown is a citizen and resident of Arkansas.

34. Plaintiff Kenneth Reagan is a citizen and resident of Missouri.

35. Plaintiffs Brown and Reagan are hereinafter referred to collectively as "Anthem Plaintiffs."

36. At all relevant times, Anthem Plaintiffs received healthcare coverage and related services from Anthem BCBS and Elevance (collectively, "Anthem"). As a condition of and in exchange for receiving healthcare coverage and services, each Anthem Plaintiff was required to provide his Private Information to Anthem, and through Anthem, to WebTPA.

Defendants

37. Defendant WebTPA Employer Services, LLC is a Texas limited liability company with its principal place of business at 8500 Freeport Parkway, suite 400, Irving, Texas 75063.

38. Defendant Hartford Life and Accident Insurance Company is a Connecticut insurance stock business engaged in business and operating in Texas and across the United States.

39. Defendant Anthem Blue Cross Life and Health Insurance Company is a California insurance stock company engaged in business and operating in Texas and across the United States.

40. Defendant Elevance Health Inc. is an Indiana corporation engaged in business and operating in Texas and across the United States.

41. Defendant Elevance is Defendant Anthem BCBS's ultimate parent company and sole beneficial owner.

42. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint if appropriate to reflect the names and capacities of other responsible parties should their identities become known.

III. JURISDICTION AND VENUE

43. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because the amount in controversy exceeds $5 million, exclusive of interest and costs, and the number of Class Members exceeds 100, many of whom have different citizenship from Defendants.

44. This Court has personal jurisdiction over WebTPA because it is incorporated and headquartered in Texas and engaged in substantial and not isolated activity in Texas.

45. This Court has personal jurisdiction over Hartford because it is engaged in

substantial and not isolated activity in Texas and has sufficient minimal conducts with this state by virtue of its engaging in business in Texas, including by collecting and/or storing Plaintiffs' and Class Members' Private Information in the state, which activities and business give rise to Plaintiffs' and Class Members' causes of action alleged herein.

46. This Court has personal jurisdiction over Anthem BCBS because it is engaged in substantial and not isolated activity in Texas and has sufficient minimal conducts with this state by virtue of its engaging in business in Texas, including by collecting and/or storing Plaintiffs' and Class Members' Private Information in the state, which activities and business give rise to Plaintiffs' and Class Members' causes of action alleged herein.

47. This Court has personal jurisdiction over Elevance because it is engaged in substantial and not isolated activity in Texas and has sufficient minimal conducts with this state by virtue of its engaging in business in Texas, including by collecting and/or storing Plaintiffs' and Class Members' Private Information in the state, which activities and business give rise to Plaintiffs' and Class Members' causes of action alleged herein.

48. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendants operate in this District and a substantial part of the events or omissions giving rise to Plaintiffs' and Class Members' claims occurred in this District, including Defendants' collecting, storing, and/or failing to secure Plaintiffs' and Class Members' Private Information.

IV. GENERAL FACTUAL ALLEGATIONS

A. Defendants Collected and Maintained Plaintiffs' and Class Members' Private Information to Operate and Facilitate their Respective Businesses.

WebTPA's Business

49. WebTPA is a third-party insurance and group benefits administrator commonly contracted by insurer clients, like Insurer Defendants, that provide group plans and related services

(among other products) to insured customers across the nation.[1]

50. WebTPA serves millions of members with 25,000 benefit plan structures, resulting in over 6.4 million claims processed by WebTPA annually.[2]

51. In order to facilitate WebTPA's services, its clients grant WebTPA access to and custody of insured customers' data, including their names, dates of birth, Social Security numbers, contact information, financial information, medical histories and treatment information, health insurance information, and other non-public, sensitive PII and PHI.

52. At all relevant times, WebTPA knew it was storing and using its networks to store and transmit valuable, sensitive Private Information and that as a result, its systems would be attractive targets for cybercriminals.

53. WebTPA also knew that any breach of its information technology network and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the millions of individuals whose Private Information was compromised, as well as intrusion into their private and sensitive personal matters.

54. As a condition of and in exchange for receiving insurance and related services, Plaintiffs and Class Members were required to entrust their highly sensitive Private Information to Insurer Defendants, and through Insurer Defendants, to WebTPA.

55. WebTPA derived economic benefits from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, WebTPA could not perform its operations, furnish the services it provides, or receive payment for those services.

---

[1] *WebTPA,* WEBTPA, https://www.webtpa.com/ (last visited May 14, 2024).
[2] *A History of Innovative Service,* WEBTPA, https://www.webtpa.com/webtpahistory (last visited May 14, 2024).

56. Indeed, WebTPA's Privacy Statement, published on its website, acknowledges that its clients' customers' Private Information is necessary "in order to operate [its] business."[3]

57. In exchange for receiving Plaintiffs' and Class Members' Private Information, WebTPA promised to safeguard the sensitive and confidential data, to use it only for authorized and legitimate purposes, and to delete such information from its systems once there was no longer a need to maintain it.

58. Upon information and belief, WebTPA made promises and representations to Insurer Defendants' customers, including Plaintiffs and Class Members, that the Private Information collected from them as a condition of obtaining products and services from Defendants, directly and indirectly, would be kept safe and confidential, that the information's privacy would be maintained, that WebTPA would delete any sensitive information after it was no longer required to maintain it.

59. Indeed, WebTPA's Privacy Statement[4] affirms and warrants in part as follows:

> WebTPA has implemented physical, electronic and technical safeguards to protect your personal information, consistent with applicable privacy and data security laws.
>
> * * *
>
> We will retain your personal information for as long as it is reasonably necessary, depending on the relevant legal and regulatory obligations and/or the duration of our business relationship with you, your employer or another related entity. . . . We will securely delete or erase your personal information if there is no valid business reason for retaining that information.

60. The information WebTPA held in its network systems at the time of the Data

[3] *WebTPA Privacy Statement*, WEBTPA, https://www.webtpa.com/privacy (last visited May 14, 2024).
[4] *WebTPA Privacy Statement*, WEBTPA, https://www.webtpa.com/privacy (last visited May 14, 2024).

Breach included the unencrypted Private Information of Plaintiffs and Class Members.

61. In addition to Insurer Defendants, a number of other WebTPA clients provided their customers' PII and/or PHI to WebTPA, which PII and/or PHI was also compromised in the Data Breach. On information and belief, these WebTPA clients include but are not limited to TransAmerica Life Insurance Company, Allied Pilots Association, American Fidelity, Dean Health Plan, Gerber Life Insurance, and Wellpoint.

Hartford's Business

62. Hartford is an insurance and benefit company and WebTPA's client, contracting with WebTPA to provide administrative services to Hartford's Group Benefits division, which includes Hartford's Critical Illness, Hospital Indemnity, Accident, Medicare Supplement and Tricare products.

63. As part of its business, Hartford collects and maintains the Private Information of millions of its current and former customer-insureds, including Hartford Plaintiffs and Class Members.

64. As a condition and in exchange for receiving insurance products and related services, Hartford Plaintiffs and Class Members were required to entrust their highly sensitive Private Information to Hartford.

65. Hartford derived economic benefits from collecting Hartford Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Hartford could not perform its operations, furnish its products and services, or generate its revenue.

66. To operate its business and facilitate WebTPA's contracted administrative services, Hartford provided Hartford Plaintiffs' and Class Members' Private Information to WebTPA.

67. At all relevant times, Hartford knew WebTPA was storing and using its networks

to store and transmit valuable, sensitive Private Information belonging to Hartford Plaintiffs and Class Members, and that as a result, WebTPA's systems would be attractive targets for cybercriminals.

68. Hartford also knew that any breach of WebTPA's information technology network and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the millions of individuals whose Private Information was compromised, as well as intrusion into those individuals' private and sensitive personal matters.

69. In exchange for receiving Hartford Plaintiffs' and Class Members' Private Information, Hartford promised to safeguard the sensitive, confidential data and ensure it was used only for authorized and legitimate purposes, to delete such information once there was no longer a need to maintain it, and to ensure the same practices from its vendors handling the Private Information, including WebTPA.

70. Indeed, Hartford's Privacy Policy,[5] published on its website, affirms and warrants in part as follows:

> HOW WE PROTECT INFORMATION
> The protection and security of your information is important to us. We work to adopt reasonable physical, administrative, and technical safeguards to protect the personal information transmitted between users and the Services and the personal information stored on our servers, and we require third parties with whom we share personal information to use reasonable precautions to safeguard such information. . . . In the event that we believe the security of your personal information in our possession or control may have been compromised, we may seek to notify you of that development. If notification is appropriate, we would endeavor to do so as promptly as possible under the circumstances[.]

[5] Online Privacy Policy, The Hartford Insurance, https://www.thehartford.com/online-privacy-policy#additional (last visited Aug. 12, 2024).

71. Moreover, Hartford's Customer Privacy Notice,[6] published on its website, affirms and warrants in part as follows:

> We value your trust. We are committed to the responsible:
> a) management;
> b) use; and
> c) protection;
> of Personal Information.
>
> * * *
>
> We only disclose Personal Health Information with:
> a) your authorization; or
> b) as otherwise allowed or required by law.
>
> Our employees have access to Personal Information in the course of doing their jobs, such as:
> a) underwriting policies;
> b) paying claims;
> c) developing new products; or
> d) advising customers of our products and services.
>
> We use manual and electronic security procedures to maintain:
> a) the confidentiality; and
> b) the integrity of;
> Personal Information that we have. We use these procedures to guard against unauthorized access.
>
> Some techniques we use to protect Personal Information include:
> a) secured files;
> b) user authentication;
> c) encryption;
> d) firewall technology; and
> e) the use of detection software.
>
> We are responsible for and must:
> a) identify information to be protected;
> b) provide an adequate level of protection for that data; and
> c) grant access to protected data only to those people who must use it in the performance of their job-related duties.

[6] Customer Privacy Notice, The Hartford Insurance, https://www.thehartford.com/customer-privacy-notice (last visited Aug. 12, 2024).

72. Additionally, Hartford's SSN Protection Policy,[7] published on its website, affirms and warrants as follows:

> We value your trust, and we are committed to the responsible protection of your Social Security number ("SSN"). This policy applies to any SSN that we collect in the course of our business. We protect the confidentiality, security and integrity of SSNs, including by implementing and maintaining administrative, technical, and physical safeguards to protect against unauthorized access to SSNs. We also limit access to SSNs, including by only granting access to SSNs to our employees who require that information to perform their job-related duties. In addition, we prohibit the disclosure of SSNs to third parties, except where required or permitted by law.

73. Upon information and belief, Hartford provided the foregoing privacy notices and policies to all customers receiving insurance and related services from Hartford, including Hartford Plaintiffs and Class Members.

Anthem's Business

74. Anthem BCBS is a life, disability, and health insurance company operating as a licensee of the Blue Cross Blue Shield Association.

75. Anthem BCBS operates across the United States, serving over 3 million members nationally. The large majority of Anthem BCBS's revenue is derived from individual and group health and accident insurance plans, with a small portion generated from its individual and group life insurance business.

76. Upon information and belief, Anthem BCBS does not have employees; employees of Elevance, Anthem BCBS's ultimate parent, provide administrative services to Anthem BCBS in connection with Anthem BCBS's insurance business, including services related to information technology and cybersecurity. In 2022, Anthem BCBS paid Elevance over $1 billion in total for

[7] SSN Protection Policy, The Hartford Insurance, https://www.thehartford.com/ssn-policy (last visited Aug. 12, 2024).

the administrative services Elevance provided to Anthem that year.

77. Upon information and belief, in providing information technology and cybersecurity services to Anthem BCBS in connection with Anthem BCBS's health insurance business, Elevance received, handled, and oversaw the data security for Anthem BCBS's insured-customers' Private Information.

78. As a condition and in exchange for receiving insurance products and related services, Anthem Plaintiffs and Class Members were required to entrust their highly sensitive Private Information to Anthem.

79. Anthem derived economic benefits from collecting Anthem Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Anthem could not perform its operations, furnish the products and services it provides, or generate its revenue.

80. To operate its business and facilitate WebTPA's contracted administrative services, Anthem provided Anthem Plaintiffs' and Class Members' Private Information to WebTPA.

81. At all relevant times, Anthem knew WebTPA was storing and using its networks to store and transmit valuable Private Information belonging to Anthem Plaintiffs and Class Members, and that as a result, WebTPA's systems would be attractive targets for cybercriminals.

82. Anthem also knew that any breach of WebTPA's information technology network and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the millions of individuals whose Private Information was compromised, as well as intrusion into those individuals' private and sensitive personal matters.

83. In exchange for receiving Anthem Plaintiffs' and Class Members' Private Information, Anthem promised to safeguard the sensitive, confidential data and ensure it was used

only for authorized and legitimate purposes, to delete such information once there was no longer a need to maintain it, and to ensure the same practices from its vendors handling the Private Information, including WebTPA.

84. Indeed, the Anthem Privacy Policy,[8] published on its website, assures its customers, "Your privacy is a priority to us, and we take great care to protect your information."[9]

85. Anthem's Personally Identifiable Information Privacy Protection Policy[10] further affirms and warrants in part as follows:

> Anthem is committed to protecting all your sensitive information in accordance with applicable laws and regulations.
>
> * * *
>
> We are committed to safeguarding the PII, PHI, and/or PI we receive from our customers and members through the use of physical, technical, and administrative safeguards.
>
> Our policies prohibit the unlawful disclosure of PII, PHI and/or PI. We share it externally only where federal and state law allows or requires it. It is our policy to limit the access, use and disclosure of this information to be in line with the job duties of our associates, as well as applicable law.

86. Anthem's HIPAA Notice of Privacy Practices[11] further promises and warrants in part as follows:

> Protecting your personal health information is important. . . . Your nonpublic (private) personal information (PI) identifies you and it's often gathered in an insurance matter. . . . We may collect, use, and share your PI as described in this notice. Our goal is to protect your

[8] Online Privacy Policy, The Hartford Insurance, https://www.thehartford.com/online-privacy-policy#additional (last visited Aug. 12, 2024).
[9] Anthem Privacy Policy, Anthem BCBS, https://www.anthem.com/privacy (last visited August 22, 2024).
[10] Personally Identifiable Information Privacy Protection Policy, Anthem BCBS https://www.anthem.com/privacy (last visited August 22, 2024).
[11] Notice of Privacy Practices, Anthem BCBS (Jan. 2024), available at https://www.anthem.com/privacy (last visited August 22, 2024).

> PI because your information can be used to make judgments about your health, finances, character, habits, hobbies, reputation, career, and credit.

87. Additionally, Anthem's HIPAA Notice of Privacy Practices states as follows:

> We're dedicated to protecting your PHI, and we've set up a number of policies and practices to help keep your PHI secure and private. If we believe your PHI has been breached, we are required to let you know. We keep your oral, written, and electronic PHI safe using the right procedures, and through physical and electronic means. These safety measures follow federal and state laws. Some of the ways we keep your PHI safe include securing offices that hold PHI, password-protecting computers, and locking storage areas and filing cabinets. We require our employees to protect PHI through written policies and procedures. These policies limit access to PHI to only those employees who need the data to do their jobs. Employees are also required to wear ID badges to help keep unauthorized people out of areas where your PHI is kept. Also, where required by law, our business partners must protect the privacy of data we share with them as they work with us. They're not allowed to give your PHI to others without your written permission, unless the law allows it and it's stated in this notice.

88. Regarding the sharing of its customers' Private Information with third parties, Anthem's HIPAA Notice of Privacy Practices further promises and warrants, "We may also share your PI with others outside our company — without your approval, in some cases. However, we take reasonable measures to protect your information."[12]

89. Anthem's HIPAA Notice of Privacy Practices further promises that the Private Information it collects will only be disclosed in specific circumstances—none of which include exposure to cybercriminals in a data breach—and that Anthem will "get your written permission before we use or share your PHI for any purpose not stated in this notice."[13]

90. Anthem's HIPAA Notice of Privacy Practices acknowledges, "Our goal is to

[12] *Id.*
[13] *Id.*

protect your PI because your information can be used to make judgments about your health, finances, character, habits, hobbies, reputation, career, and credit."[14]

91. Upon information and belief, Anthem provided the foregoing privacy notices and policies to all customers receiving insurance products and related services from Anthem, including Anthem Plaintiffs and Class Members.

B. Defendants Owed Duties to Adopt Reasonable Data Security Measures for Private Information they Collected and Maintained.

92. As part of their respective businesses, Defendants collect and maintain millions of individuals' Private Information, including that of Plaintiffs and Class Members.

93. Defendants had and continue to have duties to adopt reasonable measures to keep Plaintiffs' and Class Members' Private Information confidential and protected from disclosure to unauthorized third parties, and to audit, monitor, and verify the integrity of their IT networks and those of their vendors and affiliates.

94. Defendants' obligations stem from the Federal Trade Commission ("FTC") Act, 15 U.S.C. § 45, the Health Insurance Portability and Accountability Act ("HIPAA"), common law, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and protected from unauthorized disclosure.

95. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information. To that end, Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

96. Based on the foregoing representations and warranties and to obtain insurance products and related services from Defendants, directly or indirectly, Plaintiffs and Class Members

[14] *Id.*

provided their Private Information to Defendants with the reasonable expectation and on the mutual understanding that Defendants would comply with their promises and obligations to keep such information confidential and protected against unauthorized access.

97. Plaintiffs and Class Members relied on these promises from Defendants, and but for Defendants' promises to keep Plaintiffs' and Class Members' Private Information secure and confidential, would not have sought services from or entrusted their Private Information to Defendants. Consumers, in general, demand security for their Private Information, especially when Social Security numbers and sensitive health data are involved.

98. Additionally, by obtaining, using, and benefitting from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known they were responsible for protecting that Private Information from unauthorized access and disclosure.

99. Defendants' duty to protect Plaintiffs and Class Members from the foreseeable risk of injury that inadequate data protection and unauthorized exposure of their Private Information would case obligated Defendants to implement reasonable practices to keep Plaintiffs' and Class Members' sensitive Private Information confidential and securely maintained, to use and disclose it for necessary and authorized purposes only, to delete it from network systems when no longer necessary for legitimate business purposes, and, as to Insurer Defendants, to ensure the same data security protocols and procedures from their vendor WebTPA. Defendants failed to do so.

C. Defendants Failed to Adequately Safeguard Plaintiffs' and Class Member's Private Information, resulting in the Data Breach.

100. On or about May 8, 2024—*over a year* after the Data Breach—WebTPA began sending Plaintiffs and other Data Breach victims the Notice Letter titled "Notice of Data Breach."[15]

[15] *See* Notice Letter, Ex. A.

101. Despite their direct insurer-insured relationship with Plaintiffs and Class Members, Insurer Defendants did not send separate notifications to their customers impacted by the Data Breach, relying solely on WebTPA's Notice Letters to alert Data Breach victims.

102. The Notice Letters generally inform as follows:

> [WebTPA] recently detected a data security incident impacting certain systems on our network. We are in possession of your information because we provided administrative services to benefit plans and insurance companies, including [The Hartford/Anthem Blue Cross Life and Health Insurance Company].
>
> * * *
>
> **What happened?**
> On December 28, 2023, we detected evidence of suspicious activity on the WebTPA network that prompted us to launch an investigation. . . . The investigation concluded that the unauthorized actor may have accessed and/or obtained personal information between April 18 and April 23, 2023. WebTPA promptly informed your benefit plan or insurance company about the incident and the potential exposure of your information. We then diligently worked to confirm the individuals' impacted data and their contact information, which we provided to benefit plans and insurance companies on March 25, 2024.
>
> **What information was involved?**
> The information about you that may have been impacted includes: name, contact information, date of birth, and Social Security number.

103. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

104. Thus, Defendants' purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiffs and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms

resulting from the Data Breach is severely diminished.

105. Since receiving the Notice Letter, Plaintiffs have learned the Data Breach began on March 6, 2023, when hackers first accessed WebTPA's network through a Virtual Private Network connection, and lasted through at least May 12, 2023—without Defendants discovering the unauthorized access until *eight months* later.

106. To make matters worse, WebTPA waited over a year after the Data Breach occurred and over five months after WebTPA detected the Data Breach occurred, to begin notifying Plaintiffs and Class Members that the sensitive Private Information they entrusted to Defendants is now in criminal hackers' possession. This unreasonable and unexplained delay deprived Plaintiffs and Class Members of crucial time to address and mitigate the heightened risk of identity theft and other harms resulting from the Data Breach.

107. As the Data Breach evidences, Defendants did not use reasonable security measures appropriate to the nature of the sensitive Private Information they collected and maintained from Plaintiffs and Class Members, such as encrypting the information or deleting it when it is no longer needed, or ensuring their vendors did the same. These failures by Defendants allowed and caused cybercriminals to target WebTPA's network and carry out the Data Breach.

108. Plaintiffs' and Class Members' Private Information was targeted, accessed, and stolen by cybercriminals in the Data Breach. Criminal hackers accessed and acquired confidential files containing Plaintiffs' and Class Members' Private Information from WebTPA's network systems, where they were kept without adequate safeguards and in unencrypted form.

109. WebTPA could have prevented this Data Breach by ensuring its files and servers containing Plaintiffs' and Class Members' Private Information were properly secured, sanitized, and encrypted, but failed to do so.

110. Insurer Defendants could have prevented this Data Breach by requiring WebTPA to implement such reasonable safeguards as properly securing, sanitizing, and encrypting the files and servers containing Plaintiffs' and Class Members' Private Information, and by supervising WebTPA's data security during the course of its contracts with Insurer Defendants to ensure such reasonable safeguards were continuously maintained, but failed to do so.

111. Defendants' tortious conduct and breach of contractual obligations, as detailed in this Complaint, are evidenced by their failure to recognize the Data Breach until months after cybercriminals had breached WebTPA's network and accessed Plaintiffs' and Class Members' Private Information stored therein for weeks—meaning Defendants had no effective means in place to ensure that cyberattacks were detected and prevented.

D. Defendants Knew of the Risk of a Cyberattack because Businesses in Possession of Private Information are Particularly Suspectable.

112. Defendants' negligence in failing to safeguard Plaintiffs' and Class Members' Private Information is exacerbated by the repeated warnings and alerts regarding the need to protect and secure sensitive data.

113. Private Information of the kind accessed in the Data Breach is of great value to cybercriminals as it can be used for a variety of unlawful and nefarious purposes, including ransomware, fraudulent misuse, and sale on the internet black market known as the dark web.

114. Private Information can also be used to distinguish, identify, or trace an individual's identity, such as their name, Social Security number, and financial records. This may be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, like his or her birthdate, birthplace, or mother's maiden name.

115. Data thieves regularly target businesses in the healthcare and insurance industries like Defendants due to the highly sensitive information that such entities maintain. Defendants

knew and understood that unprotected Private Information is highly sought after by criminals who seek to illegally monetize that Private Information through unauthorized access.

116. Cyber-attacks against institutions such as Defendants are targeted and frequent. According to Contrast Security's 2023 report *Cyber Bank Heists: Threats to the financial sector*, "Over the past year, attacks have included banking trojans, ransomware, account takeover, theft of client data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."[16] In fact, "40% [of financial institutions] have been victimized by a ransomware attack."[17]

117. In light of past high profile data breaches at industry-leading companies, including, for example, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or, if acting as reasonable businesses handling PII and PHI, should have known that the Private Information they collected and maintained would be vulnerable to and targeted by cybercriminals.

118. According to the Identity Theft Resource Center's report covering the year 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017."[18]

---

[16] Contrast Security, "Cyber Bank Heists: Threats to the financial sector," pg. 5, avail. at https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%202023.pdf?hsLang=en (last visited Aug. 22, 2024).

[17] *Id.*, at 15.

[18] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," ITRC, Jan. 24, 2022, available at

119. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Defendants themselves. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[19]

120. Indeed, Anthem experienced a devastating cyberattack of its own network systems in 2015, at the time one of the largest known data breaches, resulting in the wrongful disclosure of 78.8 million individuals' PHI and PII to cybercriminals. Thus, Anthem was acutely aware of the risk of a data breach and the harm that inadequate data security measures would cause.

121. Defendants' data security obligations were particularly important given the substantial increase, preceding the date of the subject Data Breach, in cyberattacks and/or data breaches targeting entities like Defendants that collect and store PHI.

122. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims. Of the 3,205 recorded data compromises, 809 of them, or 25.2% were in the medical or healthcare industry. The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points. The 2023 compromises represent a 78 percentage point increase over the previous year and a 72 percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.

123. Entities in custody of PHI, like Defendants, reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.[20]

---

https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last visited Aug. 22, 2024).

[19] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last accessed Feb. 9, 2024).

[20] *See* Identity Theft Resource Center, 2022 Annual Data Breach Report, https://www.idtheftcenter.org/publication/2022-data-breach-report/ (last accessed May 8, 2024).

Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[21] Almost 50% of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy as a whole.[22]

124. Thus, the healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[23]

125. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

126. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even

[21] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET, March 3, 2010, available at https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited May 8, 2024).
[22] *Id.*
[23] 9 Reasons why Healthcare is the Biggest Target for Cyberattacks, Swivelsecure, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Aug. 23, 2024).

seen $60 or $70."[24] A complete identity theft kit with health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[25]

127. As businesses in possession of customers' Private Information, Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiffs and Class Members and of the foreseeable consequences if their or their vendor's network systems were breached. Such consequences include the significant costs imposed on Plaintiffs and Class Members due to a breach. Nevertheless, Defendants failed to implement or follow reasonable cybersecurity measures to protect against the Data Breach.

128. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

129. Given the nature of the Data Breach, it was foreseeable that Plaintiffs' and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiffs' and Class Members' names.

130. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on WebTPA's network server(s), amounting to millions of individuals' detailed Private Information, and, thus, that these millions of individuals would be harmed by the

[24] You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows, IDExperts, May 14, 2015, https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited Aug. 23, 2024).

[25] PriceWaterhouseCoopers, *Managing cyber risks in an interconnected world*, Sept. 30, 2014, available at https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Aug. 23, 2024).

exposure of that unencrypted data.

131. Plaintiffs and Class Members were the foreseeable and probable victims of Defendants' inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for that information.

132. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiffs and Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and the like.

E. Defendants Were Required, But Failed to Comply with FTC Rules and Guidance.

133. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

134. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*,[26] which establishes cyber-security guidelines for businesses like Defendants. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

135. The FTC's 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

[26] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM. (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Aug. 22, 2024).

the system; and have a response plan ready in the event of a breach.[27]

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

137. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect third parties' confidential 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 business like Defendant must undertake to meet their data security obligations.

138. Such FTC enforcement actions include actions against entities in the healthcare industry like Defendants. *See, e.g., In the Matter of LabMD, Inc*., 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.").

139. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendants' duties in this regard.

[27] *Id.*

140. The FTC has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[28]

141. Defendants failed to properly implement basic data security practices, in violation of their duties under the FTC Act.

142. Defendants' failures to employ reasonable and appropriate means to protect against unauthorized access to Plaintiffs' and Class Members' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by the FTC Act.

F. Defendants were Required, But Failed to Comply with HIPAA Guidelines.

143. Insurer Defendants are covered businesses under HIPAA (45 C.F.R. § 160.102) and required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160, Part 164, Subparts A and E; and Security Rule, 45 C.F.R. Part 160, Part 164, Subparts A and C.

144. Insurer Defendants are further subject to the Health Information Technology Act ("HITECH")'s rules for safeguarding electronic forms of medical information. See 42 U.S.C. §17921; 45 C.F.R. § 160.103.

145. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting PHI that is kept or transferred in electronic form.

146. HIPAA requires "compl[iance] with the applicable standards, implementation

[28] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

147. HIPAA's Security Rule required and requires that Insurer Defendants do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

148. HIPAA also required and requires Insurer Defendants to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Insurer Defendants are required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. §164.312(a)(1).

149. HIPAA and HITECH also require procedures to prevent, detect, contain, and correct data security violations and disclosures of PHI that are reasonably anticipated but not

permitted by privacy rules. See 45 C.F.R. § 164.306(a)(1), (a)(3).

150. HIPAA further requires covered entities like Insurer Defendants to have and apply appropriate sanctions against members of their 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).

151. HIPAA further requires covered entities like Insurer Defendants to mitigate, to the extent practicable, any harmful effect that is known to the entity of a use or disclosure of PHI in violation of the entity's 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).

152. 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."[29] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology, which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI."[30]

153. HIPAA's Breach Notification Rule further requires that within 60 days of discovering a breach of unsecured patient PHI, as is this Data Breach, Insurer Defendants must

[29] HHS, Security Rule Guidance Material, Aug. 21, 2024, https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited Aug. 23, 2024).
[30] HHS, Guidance on Risk Analysis, July 22, 2024, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es (last visited Aug. 23, 2024).

notify each individual affected regarding the nature of the breach, the PHI compromised, steps the individual should take to protect against potential resulting harm, and what Insurer Defendants are doing to protect against future breaches. 45 C.F.R. § 164.404(b).

154. Additionally, WebTPA is a business associate as defined under HIPAA. 45 C.F.R. § 160.103.

155. HIPAA requires that when a covered entity, like each Insurer Defendants, provides PHI to a business associate, like WebTPA, the covered entity must require by contract and ensure that the business associate uses appropriate safeguards to protect electronic PHI from unauthorized disclosure. 45 C.F.R. § 164.504(e)(2)(ii).

156. As alleged herein, Defendants violated HIPAA and HITECH. They (a) failed to maintain adequate security practices, systems, and protocols to prevent data loss, (b) failed to mitigate the risks of a data breach, (c) failed to ensure the confidentiality and protection of PHI, (d) failed to require or ensure that WebTPA used appropriate safeguards to prevent the unauthorized disclosure of Plaintiffs' and Class Members' Private Information, and (e) failed to provide the required Data Breach notice within 60 days of discovering the incident.

G. Defendants Failed to Comply with Industry Standards.

157. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

158. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability

Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.

159. In addition, the NIST recommends certain practices to safeguard systems, infra, such as the following:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices; and

g. Train everyone who uses your computers, devices, and network about cybersecurity.

160. Further still, the Cybersecurity & Infrastructure Security Agency makes specific recommendations to organizations to guard against cyberattacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior, [e]nabl[ing] logging in order to better investigate issues or events[,] and [c]onfirm[ing] that the

organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated"; (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and; (d) other steps.[31]

161. Upon information and belief, Defendants failed to implement industry standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as failing to comply with other industry standards for protecting Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

H. Defendants Owed Plaintiffs and Class Members Common Law Duties to Safeguard their Private Information.

162. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in their and/or their vendors' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. These duties owed to Plaintiffs and Class Members obligated (a) WebTPA to provide reasonable data security consistent with industry standards and requirements to protect Plaintiffs' and Class Members' Private Information in its care from unauthorized disclosure, and (b) Insurer Defendants to ensure their business associate/vendor WebTPA implemented and maintained such appropriate

[31] Cybersecurity & Infrastructure Security Agency, "Shields Up: Guidance for Organizations," available at https://www.cisa.gov/shields-guidance-organizations (last visited Feb. 9, 2024).

safeguards with respect to Plaintiffs' and Class Members' Private Information.

163. Defendants owed duties to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in their and/or their vendors' possession, including adequately training their employees and others who accessed Private Information on how to adequately protect Private Information.

164. Defendants owed duties to Plaintiffs and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

165. Defendants owed duties to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

166. Defendants owed duties to Plaintiffs and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

167. Defendants owed duties to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

168. Defendants failed to take the necessary precautions to safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure. Defendants' actions and omissions represent a flagrant disregard of Plaintiffs' and Class Members' rights.

I. Plaintiffs and Class Members Suffered Common Injuries and Damages due to Defendants' Conduct.

169. Defendants' failure to implement or maintain adequate data security measures for Plaintiffs' and Class Members' Private Information directly and proximately caused injuries to Plaintiffs and Class Members by the resulting disclosure of their Private Information in the Data Breach.

170. The ramifications of Defendants' failures to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen

fraudulent use of that information and damage to victims may continue for years.

171. Plaintiffs and Class Members are also at a continued risk because their Private Information remains in Defendants' systems, which have already been shown to be susceptible to compromise and are subject to further attack so long as Defendants fail to undertake the necessary and appropriate security and training measures to protect their customers' Private Information.

172. As a result of Defendants' ineffective and inadequate data security practices, the consequential Data Breach, and the foreseeable outcome of Plaintiffs' and Class Members' Private Information ending up in criminals' possession, all Plaintiffs and Class Members have suffered and will continue to suffer the following actual injuries and damages, without limitation: (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their Private Information; (g) loss of the benefit of their bargain with Defendants; (h) emotional distress including anxiety and stress in dealing with the Data Breach's aftermath; and (i) the continued risk to their sensitive Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information they collect and maintain.

Present and Ongoing Risk of Identity Theft

173. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

174. The FTC defines identity theft as "a fraud committed or attempted using the

identifying information of another person without authority."[32] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[33]

175. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the internet black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

176. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[34] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[35] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

177. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, PHI and PII like the Private Information at issue

[32] 17 C.F.R. § 248.201 (2013).
[33] *Id.*
[34] *What Is the dark web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[35] *Id.*

here.[36] The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[37] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[38]

178. The unencrypted Private Information of Plaintiffs and Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted and detailed Private Information may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized actors can easily access and misuse Plaintiffs' and Class Members' Private Information due to the Data Breach.

179. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

180. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social

[36] *What is the dark web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.
[37] *Id.; What Is the dark web?*, Experian, available at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.
[38] *What is the dark web?* – Microsoft 365, available at https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

181. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[39]

182. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

183. Even then, new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that

[39] Social Security Administration, *Identity Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

old bad information is quickly inherited into the new Social Security number."[40]

184. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for credit lines.[41]

185. Theft of PHI, in particular, is gravely serious as well: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[42]

186. PHI is likely to be used in detrimental ways, including by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[43]

187. Another study found "the majority [70%] of data impacted by healthcare breaches

[40] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Aug. 23, 2024).

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

[42] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Aug. 23, 2024).

[43] *Id.*

could be leveraged by hackers to commit fraud or identity theft."[44]

188. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[45]

189. "Medical identity theft is a great concern not only because of its rapid growth rate, but because it is the most expensive and time consuming to resolve of all types of identity theft. Additionally, medical identity theft is very difficult to detect which makes this form of fraud extremely dangerous."[46]

190. The reality is that cybercriminals seek nefarious outcomes from a data breach" and "stolen health data can be used to carry out a variety of crimes."[47]

191. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[48]

---

[44] DistilInfo, 70% Of Data Involved In Healthcare Breaches Increases Risk of Fraud (Oct. 3, 2019), https://distilgovhealth.com/2019/10/03/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud/ (last visited Aug. 23, 2024). .

[45] *Id.*

[46] Experian, The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches, available at https://www.experian.com/assets/databreach/white-papers/consequences-medical-id-theft-healthcare.pdf (last accessed Mar. 14, 2023). .

[47] HealthTech, What Happens to Stolen Healthcare Data?, Oct. 30, 2019, https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited Aug. 23, 2024).

[48] "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 that 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 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

192. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

193. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's 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 Private Information that was exfiltrated in the Data Breach, criminals may still 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.

194. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

195. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

196. The development of "Fullz" packages means that stolen Private Information 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. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that their stolen Private Information is being misused, and that such misuse

---

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://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm (last visited Feb. 26, 2024).

is traceable to the Data Breach.

197. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice,

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[49]

198. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[50]

199. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[51] Yet, Defendants failed to rapidly report to Plaintiffs and Class Members that their Private Information was stolen.

200. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

201. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will

[49] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Jan. 23, 2024).
[50] *See* https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.
[51] *Id.*

likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

202. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiffs and Class Members will need to remain vigilant for years or even decades to come.

Loss of Time to Mitigate the Risk of Identify Theft and Fraud

203. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the asset of time has been lost.

204. In the event that Plaintiffs and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record

205. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must monitor their financial accounts for many years to mitigate that harm.

206. Plaintiffs and Class Members have spent time, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and

filing police reports, which may take years to discover.

207. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[52]

208. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendants' conduct that caused the Data Breach.

Diminished Value of Private Information

209. Private Information is a valuable property right.[53] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

210. For example, drug and medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach

[52] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Feb. 26, 2024).

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

victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

211. Private Information can sell for as much as $363 per record according to the Infosec Institute.[54]

212. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, medical data sells on the dark web for $50 and up.

213. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[55] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[56] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[57]

214. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value for the threat actors.

215. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby

---

[54] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[55] Lazarus, D., *Shadowy data brokers make the most of their invisibility cloak*, LA TIMES (Nov. 5, 2019), available at https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[56] https://datacoup.com/.
[57] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

causing additional loss of value.

Future Cost of Credit and Identify Theft Monitoring is Reasonable and Necessary

216. To date, Defendants have done little to nothing to provide Plaintiffs and Class Members with relief for the damages they have suffered due to the Data Breach. Insurer Defendants, which had a direct relationship with Plaintiffs and Class Members, did not offer Data Breach victims even minimal compensation like temporary complimentary credit monitoring services, or even bother to notify their customers of their Private Information's unauthorized exposure in the Data Breach.

217. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money, filing false tax returns, taking out loans or lines of credit, or filing false unemployment claims.

218. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that her or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

219. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

breach, where victims can easily cancel or close credit and debit card accounts.[58] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

220. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future, if not forever.

221. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendants' failure to safeguard their Private Information.

Loss of Benefit of the Bargain

222. Furthermore, Defendants' poor data security deprived Plaintiffs and Class Members of the benefit of their bargain.

223. When agreeing to provide their Private Information, which was a condition precedent to obtain insurance and related services from Defendants, and paying Defendants, directly or indirectly, for these products and services, Plaintiffs and Class Members as consumers understood and expected that they were, in part, paying a premium for services and data security to protect the Private Information they were required to provide.

224. In fact, Defendants did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains struck with Defendants.

---

[58] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The dark web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

V. PLAINTIFFS' EXPERIENCES AND INJURIES

Hartford Plaintiffs

Plaintiff Tracy Bertocchini

225. As of condition of receiving insurance and related services from Hartford, Plaintiff Bertocchini was required to supply Hartford and WebTPA with her Private Information, including but not limited to her name, contact information, date of birth, Social Security number, health diagnosis and treatment information, health insurance information, and other sensitive information.

226. Plaintiff Bertocchini greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Bertocchini diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

227. Plaintiff Bertocchini would not have provided her Private Information to Hartford or WebTPA had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

228. At the time of the Data Breach—in or around April 2023—WebTPA retained Plaintiff Bertocchini's Private Information in its network systems with inadequate data security, causing Plaintiff Bertocchini's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

229. On or about May 8, 2024, Plaintiff Bertocchini received WebTPA's Notice Letter informing that her Private Information was accessed and exposed to unknown, unauthorized third parties through the Data Breach. According to the Notice Letter, hackers acquired files containing

Plaintiff Bertocchini's sensitive Private Information, including her name, date of birth, contact information, and Social Security number.

230. Plaintiff Bertocchini has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Bertocchini now monitors her financial and credit statements multiple times a week and has spent hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

231. Plaintiff Bertocchini's Private Information compromised in the Data Breach has already been misused by an unknown actor to make fraudulent charges to Plaintiff Bertocchini's Bank of America account, without Plaintiff Bertocchini's knowledge or authorization.

232. Due to the Data Breach and resulting fraudulent charges to her bank account, and to mitigate further harm therefrom, Plaintiff Bertocchini has cancelled her debit card and placed a credit freeze on her accounts, costing her additional time and inconvenience.

233. Plaintiff Bertocchini further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Bertocchini is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

234. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Bertocchini's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web.

235. The Data Breach has caused Plaintiff Bertocchini to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key

details about the Data Breach's occurrence or the information stolen.

236. Plaintiff Bertocchini further believes her Private Information, and that of Class Members, was and will be sold and disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

237. Moreover, Plaintiff Bertocchini has experienced suspicious spam calls and texts using the Private Information exposed in the Data Breach, and believes this be an attempt to secure additional information from or about her.

238. Other than the Data Breach, Plaintiff Bertocchini is not aware of ever being part of a data breach or similar cybersecurity incident involving her Private Information and is concerned that it has now been exposed to bad actors.

Plaintiff Mark Ellak

239. As of condition of receiving insurance and related services from Aetna, which was thereafter acquired by Hartford, Plaintiff Ellak was required to supply Hartford and WebTPA with his Private Information, including but not limited to his name, contact information, date of birth, Social Security number, health diagnosis and treatment information, health insurance information, and other sensitive information.

240. Plaintiff Ellak greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Ellak diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

241. Plaintiff Ellak would not have provided his Private Information to Hartford or WebTPA had he known it would be kept using inadequate data security and vulnerable to a

cyberattack.

242. At the time of the Data Breach—in or around April 2023—WebTPA retained Plaintiff Ellak's Private Information in its network systems with inadequate data security, causing Plaintiff Ellak's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

243. On or about May 8, 2024, Plaintiff Ellak received WebTPA's Notice Letter informing that his Private Information was accessed and exposed to unknown, unauthorized third parties through the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Ellak's sensitive Private Information, including his name, date of birth, contact information, and Social Security number.

244. Plaintiff Ellak has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Ellak now monitors his financial and credit statements multiple times a week and has already spent over 7 hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

245. Plaintiff Ellak further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Ellak is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

246. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Burger's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web following the Data Breach.

247. Plaintiff Ellak further believes his Private Information, and that of Class Members, was and will be sold and further disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

248. The Data Breach has caused Plaintiff Ellak to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence or the information stolen. Plaintiff Ellak has suffered and continues to suffer anxiety and fear about the genuine and materialized risk that he will be the victim of identity theft due to his Private Information's exposure in the Data Breach.

249. Moreover, following the Data Breach, Plaintiff Ellak has experienced suspicious spam calls, texts, and emails using the Private Information exposed in the Data Breach, giving rise to further anxiety and stress that his Private Information is now in the hands of bad actors.

250. Other than the Data Breach, Plaintiff Ellak is not aware of ever being part of a data breach or similar cybersecurity incident involving his Private Information and is concerned that it has now been exposed to bad actors.

Plaintiff Cory France

251. As of condition of receiving insurance and related services from Hartford, Plaintiff France was required to supply Hartford and WebTPA with his Private Information, including but not limited to his name, contact information, date of birth, Social Security number, health diagnosis and treatment information, health insurance information, and other sensitive information.

252. Plaintiff France greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff France diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other

unsecured source.

253. Plaintiff France would not have provided his Private Information to Hartford or WebTPA had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

254. At the time of the Data Breach—in or around April 2023—WebTPA retained Plaintiff France's Private Information in its network systems with inadequate data security, causing Plaintiff France's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

255. On or about May 8, 2024, Plaintiff France received WebTPA's Notice Letter informing that his Private Information was accessed and exposed to unknown, unauthorized third parties through the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff France's sensitive Private Information, including his name, date of birth, contact information, and Social Security number.

256. Plaintiff France has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff France now monitors his financial and credit statements multiple times a week and has already spent nearly 100 hours investigating the Data Breach and dealing with its effects, valuable time he otherwise would have spent on other activities.

257. Plaintiff France further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff France is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

258. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff France's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web following the Data Breach.

259. Following the Data Breach, Plaintiff France received a notification from his credit monitoring service that his Private Information compromised in the Data Breach was found published on the dark web.

260. Additionally, Plaintiff France's Private Information compromised in the Data Breach has already been misused by an unknown actor to fraudulently take out unemployment benefits in Iowa under Plaintiff France's name, without his knowledge or authorization.

261. The Data Breach has caused Plaintiff France to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence or the information stolen. Plaintiff France has suffered and continues to suffer anxiety and fear that his Private Information will be used misused. While Plaintiff France signed up for the temporary credit monitoring service offered by WebTPA, he fears what will happen after his data protection period ends. Moreover, Plaintiff France is anxious and fearful as to how the Data Breach and compromise of his Private Information will impact his children's lives, and he has taken extra steps to protect his kids' privacy.

262. Plaintiff France further believes his Private Information, and that of Class Members, was and will be sold and further disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

263. Moreover, following the Data Breach, Plaintiff France has experienced suspicious spam calls and texts using the Private Information exposed in the Data Breach, and believes this be an attempt to secure additional information from or about him.

264. Other than the Data Breach, Plaintiff France is not aware of ever being part of a data breach or similar cybersecurity incident involving his Private Information and is concerned that it has now been exposed to bad actors.

Plaintiff Chandra Chang

265. As of condition of receiving insurance and related services from Hartford, Plaintiff Chang was required to supply Hartford and WebTPA with her Private Information, including but not limited to her name, contact information, date of birth, Social Security number, health diagnosis and treatment information, health insurance information, and other sensitive information.

266. Plaintiff Chang greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Chang diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

267. Plaintiff Chang would not have provided her Private Information to Hartford or WebTPA had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

268. At the time of the Data Breach—in or around April 2023—WebTPA retained Plaintiff Chang's Private Information in its network systems with inadequate data security, causing Plaintiff Chang's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

269. On or about May 8, 2024, Plaintiff Chang received WebTPA's Notice Letter informing that her Private Information was accessed and exposed to unknown, unauthorized third

parties through the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Chang's sensitive Private Information, including her name, date of birth, contact information, and Social Security number.

270. Plaintiff Chang has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Chang now monitors her financial and credit statements multiple times a week and spends about one hour per week dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

271. After the Data Breach, Plaintiff Chang was notified by her credit monitoring service that her Private Information compromised in the Data Breach was found posted on the dark web.

272. In addition, Plaintiff Chang's Private Information compromised in the Data Breach was misused in or around June of 2024, when Plaintiff Chang received a notification regarding a fraudulent account inquiry an unknown actor made in Plaintiff Chang's name, without her knowledge or authorization.

273. Due to the Data Breach and to mitigate further harm therefrom, Plaintiff Chang has placed a credit freeze on her accounts and had a new debit card issued.

274. Plaintiff Chang further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Chang is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

275. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Chang's and Class Members' Private Information was targeted, accessed, misused,

and disseminated on the dark web.

276. The Data Breach has caused Plaintiff Chang to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence or the information stolen.

277. Plaintiff Chang further believes her Private Information, and that of Class Members, was and will be sold and further disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

278. Moreover, following the Data Breach, Plaintiff Chang has experienced suspicious spam calls and texts using the Private Information exposed in the Data Breach, and believes this be an attempt to secure additional information from or about her.

279. Other than the Data Breach, Plaintiff Chang is not aware of ever being part of a data breach or similar cybersecurity incident involving her Private Information and is concerned that it has now been exposed to bad actors.

Plaintiff Conrad Heller

280. As of condition of receiving insurance and related services from Hartford, Plaintiff Heller was required to supply Hartford and WebTPA with his Private Information, including but not limited to his name, contact information, date of birth, Social Security number, health diagnosis and treatment information, health insurance information, and other sensitive information.

281. Plaintiff Heller greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Heller diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

282. Plaintiff Heller would not have provided his Private Information to Hartford or WebTPA had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

283. At the time of the Data Breach—in or around April 2023—WebTPA retained Plaintiff Heller's Private Information in its network systems with inadequate data security, causing Plaintiff Heller's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

284. On or about May 8, 2024, Plaintiff Heller received WebTPA's Notice Letter informing that his Private Information was accessed and exposed to unknown, unauthorized third parties through the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Heller's sensitive Private Information, including his name, date of birth, contact information, and Social Security number. As Plaintiff Heller has received an uptick in suspicious correspondence and charges with his specific medical information following the Data Breach, he believes his PHI was compromised as well.

285. Plaintiff Heller has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Heller now monitors his financial and credit statements multiple times a week and has already spent over 50 hours dealing with the Data Breach's effects, valuable time he otherwise would have spent on other activities.

286. Plaintiff Heller further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data

Breach, Plaintiff Heller is at a present risk and will continue to be at increased risk of identity theft and fraud for years.

287. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Heller's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web following the Data Breach.

288. Following the Data Breach, Plaintiff Heller's Private Information compromised therein has already been misused, evidenced by fraudulent charges on his debit card for Amazon Prime Video, which Plaintiff Heller did not authorize. As a result, Plaintiff Heller closed his bank account and opened a new one, costing him $15.00, and closed his credit card as well.

289. Due to needing a new debit card, Plaintiff Heller had to spend time resetting his automatic billing information for his electric bills. After Plaintiff Heller reset the automatic billing information for his electricity, he received a higher charge on his bill from the electric company. Now, Plaintiff Heller closely monitors his bill and does not use automatic payments.

290. Moreover, following the Data Breach, Plaintiff Heller received correspondence stating that he owes money to a medical facility where he did not receive any treatment or services. The bills are addressed to Plaintiff Heller from a clinic called Patient First, which he has never been to, although he does visit a clinic called Family First. Thus, either these bills are completely sham charges using Plaintiff Heller's Private Information exposed in the Data Breach, or an unknown actor is fraudulently using Plaintiff Heller's compromised Private Information to obtain medical services.

291. The Data Breach has caused Plaintiff Heller to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence or the information stolen. Plaintiff Heller has suffered

and continues to suffer anxiety and fear that cybercriminals will steal his credit card information, and worries he will have to change his phone number soon.

292. Plaintiff Heller further believes his Private Information, and that of Class Members, was and will be sold and further disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

293. Moreover, Plaintiff Heller has experienced suspicious spam calls and texts using the Private Information exposed in the Data Breach—often up to 100 spam calls per day. As Plaintiff Heller is a self-employed stylist, the influx of spam calls is highly disruptive and inconvenient since he must answer all unknown numbers in case a potential client is trying to reach out to him.

294. Other than the Data Breach, Plaintiff Heller is not aware of ever being part of a data breach or similar cybersecurity incident involving his Private Information and is concerned that it has now been exposed to bad actors.

Plaintiff Sofia Bersineva

295. As of condition of receiving insurance and related services from Hartford, Plaintiff Bersineva was required to supply Hartford and WebTPA with her Private Information, including but not limited to her name, contact information, date of birth, Social Security number, health diagnosis and treatment information, health insurance information, and other sensitive information.

296. Plaintiff Bersineva greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Bersineva diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never

knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

297. Plaintiff Bersineva would not have provided her Private Information to Hartford or WebTPA had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

298. At the time of the Data Breach—in or around April 2023—WebTPA retained Plaintiff Bersineva's Private Information in their network systems with inadequate data security, causing Plaintiff Bersineva's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

299. On or about May 8, 2024, Plaintiff Bersineva received WebTPA's Notice Letter informing that her Private Information was accessed and exposed to unknown, unauthorized third parties through the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Bersineva's sensitive Private Information, including her name, date of birth, contact information, and Social Security number.

300. In January 2024, Credit Karma notified Plaintiff Bersineva that her Private Information compromised in the Data Breach was found posted on the dark web.

301. Plaintiff Bersineva's Private Information compromised in the Data Breach has already been misused by unauthorized actors, evidenced by an alert she received from her credit card company in December 2023 regarding a suspicious charge attempted on her account.

302. Plaintiff Bersineva has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Berseneva now monitors her financial and credit statements multiple times a week and

has already spent hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

303. Additionally, due to the fraudulent charge attempted to her credit card, Plaintiff Bersineva had a credit freeze placed on her accounts, depriving her of access to her credit (and valuable credit card benefits and awards) and causing additional lost time and inconvenience.

304. Plaintiff Bersineva further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Berseneva is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

305. The risk of identity theft is impending and materialized, as there is evidence that Plaintiff Bersineva's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web.

306. The Data Breach has caused Plaintiff Bersineva to suffer fear, anxiety, and stress—particularly about identity theft—which is compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence or the information stolen.

307. Plaintiff Bersineva further believes her Private Information, and that of Class Members, was and will be sold and further disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

308. Moreover, following the Data Breach, Plaintiff Bersineva has experienced suspicious spam calls and texts using the Private Information exposed in the Data Breach, and believes this be an attempt to secure additional information from or about her.

309. Other than the Data Breach, Plaintiff Bersineva is not aware of ever being part of a similar cybersecurity incident involving her Private Information exposed in this Data Breach.

Plaintiff Heavenle Wood

310. As of condition of receiving insurance and related services from Hartford, Plaintiff Wood was required to supply Hartford and WebTPA with her Private Information, including but not limited to her name, contact information, date of birth, Social Security number, health diagnosis and treatment information, health insurance information, and other sensitive information.

311. Plaintiff Wood greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Wood diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

312. Plaintiff Wood would not have provided her Private Information to Hartford or WebTPA had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

313. At the time of the Data Breach—in or around April 2023—WebTPA retained Plaintiff Wood's Private Information in its network systems with inadequate data security, causing her Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

314. On or about May 8, 2024, Plaintiff Wood received WebTPA's Notice Letter informing that her Private Information was accessed and exposed to unknown, unauthorized third parties through the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Wood's sensitive Private Information, including her name, date of birth, contact information, and Social Security number. Based on suspicious calls and correspondence related to health insurance that Plaintiff Wood has received following the Data Breach, her PHI was likely

compromised in the Data Breach as well.

315. Following the Data Breach, Plaintiff Wood received an email notifying that her Private Information compromised in the Data Breach was found posted on the dark web.

316. Plaintiff Wood has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Wood now monitors her financial and credit statements multiple times a week and has already spent hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

317. Plaintiff Wood further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Wood is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

318. The risk of identity theft is impending and materialized, as there is evidence that Plaintiff Wood's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web.

319. The Data Breach has caused Plaintiff Wood to suffer fear, anxiety, and stress—particularly about identity theft and the loss of control over her Private Information, given that she is typically very cautious regarding its security.

320. Plaintiff Wood further believes her Private Information, and that of Class Members, was and will be sold and further disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

321. Moreover, following the Data Breach, Plaintiff Wood has experienced suspicious

spam calls and texts using the Private Information exposed in the Data Breach, often offering her health insurance or Medicare enrollment, and believes this be an attempt to secure additional information from or about her.

322. Other than the Data Breach, Plaintiff Wood is not aware of ever being part of a data breach or similar cybersecurity incident involving her Private Information and is concerned that it has now been exposed to bad actors.

Plaintiff Cynthia Austing

323. As of condition of receiving insurance and related services from Hartford, Plaintiff Austing was required to supply Hartford and WebTPA with her Private Information, including but not limited to her name, contact information, date of birth, Social Security number, health diagnosis and treatment information, health insurance information, and other sensitive information.

324. Plaintiff Austing greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Austing diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

325. Plaintiff Austing would not have provided her Private Information to Hartford or WebTPA had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

326. At the time of the Data Breach—in or around April 2023—WebTPA retained Plaintiff Austing's Private Information in its network systems with inadequate data security, causing Plaintiff Austing's Private Information to be accessed and exfiltrated by cybercriminals in

the Data Breach.

327. On or about May 8, 2024, Plaintiff Austing received WebTPA's Notice Letter informing that her Private Information was accessed and exposed to unknown, unauthorized third parties through the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Austing's sensitive Private Information, including her name, date of birth, contact information, and Social Security number.

328. Plaintiff Austing has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Austing now monitors her financial and credit statements multiple times a week and spends about one hour per week dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

329. In response to the Data Breach and Defendants' Notice Letter, Plaintiff Austing enrolled in credit monitoring services, which notified her twice that her Private Information was found posted on the dark web.

330. In addition, Plaintiff Austing's Private Information compromised in the Data Breach was misused in or around April of 2024 by an unknown actor in China to purchase a $300 backpack using Plaintiff Austing's credit, without her authorization.

331. Plaintiff Austing further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Austing is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

332. The risk of identity theft is impending and has materialized, as there is evidence

that Plaintiff Austing's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web.

333. The Data Breach has caused Plaintiff Austing to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence or the information stolen.

334. Plaintiff Austing further believes her Private Information, and that of Class Members, was and will be sold and further disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

335. Moreover, following the Data Breach, Plaintiff Austing has experienced suspicious spam calls and texts using the Private Information exposed in the Data Breach, and believes this be an attempt to secure additional information from or about her.

336. Other than the Data Breach, Plaintiff Austing is not aware of ever being part of a data breach or similar cybersecurity incident involving her Private Information and is concerned that it has now been exposed to bad actors.

Plaintiff Belinda Gullette

337. As of condition of receiving insurance and related services from Hartford, Plaintiff Gullette was required to supply Hartford and WebTPA with her Private Information, including but not limited to her name, contact information, date of birth, Social Security number, health diagnosis and treatment information, health insurance information, and other sensitive information.

338. Plaintiff Gullette greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Gullette diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never

knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

339. Plaintiff Gullette would not have provided her Private Information to Hartford or WebTPA had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

340. At the time of the Data Breach—in or around April 2023—WebTPA retained Plaintiff Gullette's Private Information in its network systems with inadequate data security measures, causing Plaintiff Gullette's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

341. On or about May 8, 2024, Plaintiff Gullette received WebTPA's Notice Letter informing that her Private Information was accessed and exposed to unknown, unauthorized third parties through the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff's sensitive Private Information, including her name, date of birth, contact information, and Social Security number.

342. Plaintiff Gullette has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Gullette now monitors her financial and credit statements multiple times a week and has already spent many hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

343. In response to the Data Breach and the Notice Letter, Plaintiff Gullette enrolled in credit monitoring services and was notified that her Private Information is posted on the dark web.

344. Plaintiff Gullette further anticipates spending considerable time and money on an

ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Gullette is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

345. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Gullette's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web.

346. The Data Breach has caused Plaintiff Gullette to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence or the information stolen.

347. Plaintiff Gullette further believes her Private Information, and that of Class Members, was and will be sold and further disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

348. Moreover, following the Data Breach, Plaintiff Gullette has experienced suspicious spam calls and texts using the Private Information exposed in the Data Breach, and believes this be an attempt to secure additional information from or about her.

349. Other than the Data Breach, Plaintiff Gullette is not aware of ever being part of a data breach or similar cybersecurity incident involving her Private Information that was exposed in this Data Breach and is concerned that it has now been exposed to bad actors.

Plaintiff Chanelle Zimmerman

350. As of condition of receiving insurance and related services from Hartford, Plaintiff Zimmerman was required to supply Hartford and WebTPA with her Private Information, including but not limited to her name, contact information, date of birth, Social Security number, health diagnosis and treatment information, health insurance information, and other sensitive

information.

351. Plaintiff Zimmerman greatly values her privacy and is very careful about sharing her sensitive Private Information. Plaintiff Zimmerman diligently protects her Private Information and stores any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

352. Plaintiff Zimmerman would not have given her Private Information to Hartford or WebTPA had she known it would be kept using inadequate data security and vulnerable to a cyberattack.

353. At the time of the Data Breach—in or around April 2023—WebTPA retained Plaintiff Zimmerman's Private Information in its network systems with inadequate data security, causing Plaintiff Zimmerman's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

354. On or about May 8, 2024, Plaintiff Zimmerman received WebTPA's Notice Letter informing that her Private Information was accessed and exposed to unknown, unauthorized third parties through the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Zimmerman's sensitive Private Information, including her name, date of birth, contact information, and Social Security number.

355. Plaintiff Zimmerman has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Zimmerman now monitors her financial and credit statements multiple times a week and has already spent hours dealing with the Data Breach, valuable time she otherwise would have

spent on other activities.

356. Since the Data Breach, Experian has notified Plaintiff Zimmerman three times (April 10, 2024, May 6, 2024, and June 4, 2024) that her Private Information compromised in the Data Breach is posted on the dark web.

357. In addition, Plaintiff Zimmerman's Private Information compromised in the Data Breach was misused in or around December 2023, when an unknown actor attempted to take out a line of credit with Discover in Plaintiff Zimmerman's name, without her knowledge or authorization. Plaintiff Zimmerman learned of this fraud when Discover sent her a letter denying the line of credit, on or about December 13, 2023.

358. Plaintiff Zimmerman further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Zimmerman is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

359. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Zimmerman's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web.

360. The Data Breach has caused Plaintiff Zimmerman to suffer fear, anxiety, and stress—particularly that she will be a recurring victim of identity theft—which is compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence or the information stolen.

361. Plaintiff Zimmerman further believes her Private Information, and that of Class Members, was and will be sold and further disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

362. Moreover, following the Data Breach, Plaintiff Zimmerman has experienced suspicious spam calls and texts using the Private Information exposed in the Data Breach, and believes this be an attempt to secure additional information from or about her.

363. Other than the Data Breach, Plaintiff Zimmerman is not aware of ever being part of a data breach or similar cybersecurity incident involving her Private Information and is concerned that it has now been exposed to bad actors.

Plaintiff Leonard Finkel

364. As of condition of receiving insurance and related services from Hartford, Plaintiff Finkel was required to supply Hartford and WebTPA with his Private Information, including but not limited to his name, contact information, date of birth, Social Security number, health diagnosis and treatment information, health insurance information, and other sensitive information.

365. Plaintiff Finkel greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Finkel diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

366. Plaintiff Finkel would not have provided his Private Information to Hartford or WebTPA had he known it would be kept using inadequate data security and vulnerable to a cyberattack.

367. At the time of the Data Breach—in or around April 2023—WebTPA retained Plaintiff Finkel's Private Information in its network systems with inadequate data security, causing Plaintiff Finkel's Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

368. On or about June 24, 2024, Plaintiff Finkel received WebTPA's Notice Letter informing that his Private Information was accessed and exposed to unknown, unauthorized third parties through the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Finkel's sensitive Private Information, including his name, date of birth, contact information, and Social Security number. Based on the uptick in spam calls and texts referring to Mr. Finkel's specific health issues he has experienced since the Data Breach, Mr. Finkel believes his PHI was exposed in the Data Breach as well.

369. Plaintiff Finkel has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Heller now monitors his financial and credit statements multiple times a week and has already spent over 50 hours dealing with the Data Breach's effects, valuable time he otherwise would have spent on other activities.

370. Plaintiff Finkel further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Finkel is at a present risk and will continue to be at increased risk of identity theft and fraud for years.

371. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Finkel's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web following the Data Breach.

372. Following the Data Breach, Plaintiff Finkel's Private Information compromised therein has already been misused, evidenced by recurring issues with undelivered Social Security checks that Mr. Finkel has experienced over the past year, and a suspicious letter from the IRS

confirming information was submitted that Plaintiff Finkel did not recognize.

373. Moreover, following the Data Breach Plaintiff Finkel has experienced an uptick in suspicious robocalls and spam texts related to his specific health and medical matters.

374. The Data Breach has caused Plaintiff Finkel to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence or the information stolen. Plaintiff Finkel has suffered and continues to suffer anxiety that cybercriminals have his financial and health information.

375. Plaintiff Finkel further believes his Private Information, and that of Class Members, was and will be sold and further disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

Anthem Plaintiffs

Plaintiff Michael Brown

376. As of condition of receiving insurance and related services from Anthem, Plaintiff Brown was required to supply Anthem and WebTPA with his Private Information, including but not limited to his name, contact information, date of birth, Social Security number, health diagnosis and treatment information, health insurance information, and other sensitive information.

377. Plaintiff Brown greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Brown diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

378. Plaintiff Brown would not have provided his Private Information to Anthem or WebTPA had he known it would be kept using inadequate data security and vulnerable to a

cyberattack.

379. At the time of the Data Breach—in or around April 2023—WebTPA retained Plaintiff Brown's Private Information in its network systems with inadequate data security, causing his Private Information to be accessed and exfiltrated by cybercriminals in the Data Breach.

380. On or about May 8, 2024, Plaintiff Brown received WebTPA's Notice Letter informing that his Private Information was accessed and exposed to unknown, unauthorized third parties through the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Brown's sensitive Private Information, including his name, date of birth, contact information, and Social Security number.

381. Plaintiff Brown has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Brown now monitors his financial and credit statements multiple times a week and has already spent hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

382. Plaintiff Brown further anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Brown is at a present risk and will continue to be at an increased risk of identity theft and fraud for years to come. Plaintiff Brown has enrolled in a credit monitoring service from Norton 360 for an annual cost of $150.00, which he anticipates having to pay for years, if not the rest of his lifetime, due to his Private Information's exposure in the Data Breach and the attendant ongoing and imminent risk of identity theft now facing him.

383. The risk of identity theft is impending and has materialized, as there is evidence

that Plaintiff Brown's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web following the Data Breach.

384. Plaintiff Brown further believes his Private Information, and that of Class Members, was and will be sold and further disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

385. The Data Breach has caused Plaintiff Brown to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence or the information stolen. Plaintiff Brown has suffered and continues to suffer anxiety and fear about the genuine and materialized risk that his Private Information exposed in the Data Breach will be used to steal his identity. Plaintiff Brown is particularly concerned about criminals accessing and using his minor children's PII and PHI, which was also compromised in the Data Breach, and has suffered substantial and continuous anxiety and stress about the lasting impact the Data Breach will have on his children.

386. Moreover, following the Data Breach, Plaintiff Brown has experienced suspicious spam calls, texts, and emails using the Private Information exposed in the Data Breach.

387. Plaintiff Brown is not aware of ever being part of a data breach or similar cybersecurity incident involving his Private Information prior to the Data Breach, and is concerned that it has now been exposed to bad actors.

Plaintiff Kenneth Reagan

388. As of condition of receiving insurance and related services from Anthem, Plaintiff Reagan was required to supply Anthem and WebTPA with his Private Information, including but not limited to his name, contact information, date of birth, Social Security number, health diagnosis and treatment information, health insurance information, and other sensitive information.

389. Plaintiff Reagan greatly values his privacy and is very careful about sharing his sensitive Private Information. Plaintiff Reagan diligently protects his Private Information and stores any documents containing Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

390. Plaintiff Reagan would not have provided his Private Information to Anthem or WebTPA had he known it would kept using inadequate data security and vulnerable to a cyberattack.

391. At the time of the Data Breach—in or around April 2023—WebTPA retained Plaintiff Reagan's Private Information in its network systems with inadequate security, causing it to be accessed and exfiltrated by cybercriminals in the Data Breach.

392. On or about May 8, 2024, Plaintiff Reagan received WebTPA's Notice Letter informing that his Private Information was accessed and exposed to unknown, unauthorized third parties through the Data Breach. According to the Notice Letter, hackers acquired files containing Plaintiff Reagan's sensitive Private Information, including his name, date of birth, contact information, and Social Security number. Plaintiff Reagan believes his PHI was exposed in the Data Breach as well.

393. Plaintiff Reagan has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and account statements for any indications of identity theft or fraud. Plaintiff Reagan now monitors his financial and credit statements multiple times a week and has already spent hours dealing with the Data Breach's effects, valuable time he otherwise would have spent on other activities.

394. Plaintiff Reagan further anticipates spending considerable time and money on an

ongoing basis to try to mitigate and address harms caused by the Data Breach. Due to the Data Breach, Plaintiff Reagan is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

395. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Reagan's and Class Members' Private Information was targeted, accessed, misused, and disseminated on the dark web following the Data Breach.

396. As a result of the Data Breach, Plaintiff Reagan's Private Information has been posted on the dark web. On or around February 7, 2024, Plaintiff Reagan received a notification from Google that his Private Information was found on the dark web. On or around April 15, 2024, Plaintiff Reagan's credit monitoring company again informed that his Private Information was found on the dark web.

397. In January 2024, Plaintiff Reagan's Private Information compromised in the Data Breach was used by an unknown actor to attempt a $2.55 charge to Plaintiff Reagan's debit card from India, without Plaintiff Reagan's authorization. When Plaintiff Reagan's bank notified him about the suspicious transaction he cancelled his debit card and had a new one reissued, but he worries that is not enough to protect against further identity theft.

398. Moreover, Plaintiff Reagan has experienced suspicious spam calls and texts using the Private Information exposed in the Data Breach and believes this be an attempt to secure additional information from or about him. These include an influx of spam calls, texts, and emails regarding Plaintiff Reagan's private medical conditions and supplies and treatments for them. Plaintiff Reagan did not receive such communications before the Data Breach.

399. As a result of the Data Breach, Plaintiff Reagan has suffered and continues to suffer anxiety and fear that his Private Information, especially his confidential medical history, is now

open to the public and any nefarious actor who wants it.

400. Plaintiff Reagan further believes his Private Information, and that of Class Members, was and will be sold and further disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyberattacks of this type.

401. Other than the Data Breach, Plaintiff Reagan is not aware of ever being part of a data breach or similar cybersecurity incident involving his Private Information.

VI. CLASS ACTION ALLEGATIONS

402. Plaintiffs bring this nationwide class action on behalf of themselves and others similarly situated pursuant to Federal Rule of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4).

403. Plaintiffs propose the following nationwide class definition, subject to amendment based on information obtained through discovery:

> All persons in the United States whose Private Information was compromised in the Data Breach, including all persons who received a Notice Letter ("Nationwide Class").

404. Pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3), and (c)(4), as appropriate, Plaintiffs seek certification of state common law claims in the alternative to the nationwide claims, as well as statutory claims under state data breach and/or consumer protection statutes, on behalf of subclasses for residents of Arkansas, California, Florida, Georgia, Illinois, Missouri, New York, North Carolina, Ohio, and Pennsylvania (collectively, "State Subclasses") (for purposes of this Section VI, Nationwide Class and State Subclasses collectively, "Classes").

405. Each State Subclass is defined as follows:

Arkansas Subclass

> All residents of Arkansas whose Private Information was compromised in the Data Breach, including all persons who received a Notice Letter.

California Subclass

All residents of California whose Private Information was compromised in the Data Breach, including all persons who received a Notice Letter.

Florida Subclass

All residents of Florida whose Private Information was compromised in the Data Breach, including all persons who received a Notice Letter.

Georgia Subclass

All residents of Georgia whose Private Information was compromised in the Data Breach, including all persons who received a Notice Letter.

Illinois Subclass

All residents of Georgia whose Private Information was compromised in the Data Breach, including all persons who received a Notice Letter.

Missouri Subclass

All residents of Missouri whose Private Information was compromised in the Data Breach, including all persons who received a Notice Letter.

New York Subclass

All residents of New York whose Private Information was compromised in the Data Breach, including all persons who received a Notice Letter.

North Carolina Subclass

All residents of New York whose Private Information was compromised in the Data Breach, including all persons who received a Notice Letter.

Ohio Subclass

All residents of Ohio whose Private Information was compromised in the Data Breach, including all persons who received a Notice Letter.

Pennsylvania Subclass

> All residents of Pennsylvania whose Private Information was compromised in the Data Breach, including all persons who received a Notice Letter.

406. Excluded from the Classes are the following individuals and/or entities: Defendants and each Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which any Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

407. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

408. **Numerosity:** Each of the Classes is so numerous that joinder of all members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, WebTPA has reported that the Private Information of at least 2,492,175 individuals throughout the United States was compromised in the Data Breach. Upon information and belief, there are at least thousands of members in each State Subclass, making joinder of all members of the State Subclasses impractical.

409. **Commonality:** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiffs and Class Members;

c. Whether Defendants had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

d. Whether Defendants had duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

e. Whether Insurer Defendants had duties to supervise their business associates'/vendors' data security for Private Information;

f. Whether Defendants knew or should have known of the data security vulnerabilities that allowed the Data Breach to occur;

g. Whether Insurer Defendants knew or should have known of the risks to Plaintiffs' and Class Members' Private Information in WebTPA's custody;

h. Whether Defendants failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

i. Whether WebTPA's data security systems prior to, during, and since the Data Breach complied with industry standards;

j. When Defendants actually learned of the Data Breach;

k. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members their Private Information had been compromised;

l. Whether Defendants violated data breach notification laws by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

m. Whether Defendants' conduct violated the FTC Act, HIPAA, and/or HITECH;

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

o. Whether Defendants adequately addressed and fixed the vulnerabilities that permitted the Data Breach to occur;

p. Whether Defendants engaged in unfair, unlawful, or deceptive practice by failing to safeguard the Private Information of Plaintiffs and Class Members;

q. Whether Defendants engaged in unfair, unlawful, or deceptive practice by concealing and/or misrepresenting WebTPA's data security processes and vulnerabilities;

r. Whether Defendants were unjustly enriched by failing to provide adequate security for Plaintiffs' and Class Members' Private Information;

s. Whether Plaintiffs and Class Members are entitled to actual, consequential, nominal, statutory, and/or punitive damages as a result of Defendants' wrongful conduct;

t. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

u. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm the Data Breach caused.

410. **Typicality:** As to each of the Classes, Plaintiffs' claims are typical of other Class Members' claims because Plaintiffs and Class Members were subject to the same unlawful conduct as alleged herein, and were damaged in the same way. Plaintiffs' Private Information was in Defendants' possession at the time of the Data Breach and was compromised due to the Data Breach. Plaintiffs' damages and injuries are akin to those of other Class Members and Plaintiffs seek relief consistent with the relief of the Classes.

411. **Adequacy:** Plaintiffs are adequate representatives of the Classes because Plaintiffs are all members of the Nationwide Class, and respectively members of the State Subclasses, and are committed to pursuing this matter against Defendants to obtain relief for the Classes. Plaintiffs

have no conflicts of interest with the Classes. Plaintiffs' Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the interests of all the Classes.

412. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to Plaintiffs and Class Members may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and Class Members are relatively small compared to the burden and expense required to individually litigate their claims against Defendants, and thus, individual litigation to redress Defendants' wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

413. **Manageability:** The litigation of the class claims alleged herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates there would be no significant manageability problems with prosecuting this lawsuit as a class action. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

414. **Ascertainability:** All members of the proposed Classes are readily ascertainable. The Classes are defined by reference to objective criteria, and there is an administratively feasible

mechanism to determine who fits within the Classes. Defendants have access to information regarding the individuals affected by the Data Breach, and WebTPA has already provided notifications to some or all of those people. Using this information, the members of the Classes can be identified, and their contact information ascertained for purposes of providing notice.

415. **Particular Issues:** Particular issues are appropriate for certification under Rule 23(c)(4) 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 the following:

a. Whether Defendants owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Insurer Defendants on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Insurer Defendants breached the implied contract;

f. Whether Defendants adequately and accurately informed Plaintiffs and Class Members their Private Information had been compromised;

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

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to

safeguard the Private Information of Plaintiffs and Class Members; and

i. Whether Class Members are entitled to actual, consequential, statutory, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

416. **Policies Generally Applicable to the Classes:** Finally, class certification is also appropriate under Rule 23(b)(2) and (c). Each of the Classes are also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to each of the Classes as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly, and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

417. Defendants, through uniform conduct, acted or refused to act on grounds generally applicable to the Classes as a whole, making injunctive and declaratory relief appropriate to the Classes as a whole, including without limitation the following:

a. Ordering Defendants to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Ordering that, to comply with Defendants' explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain, and must require their vendors handling Private Information to implement and maintain, reasonable security and monitoring measures, including, but not limited to the following:

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

ii. requiring Defendants to protect, including through encryption, all data collected

through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete and purge the Private Information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

v. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis;

vi. prohibiting Defendants from maintaining Private Information on a cloud-based database until proper safeguards and processes are implemented;

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

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

ix. requiring Defendants to monitor ingress and egress of all network traffic;

x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as

protecting the Private Information of Plaintiffs and Class Members;

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

xii. requiring Defendants to meaningfully educate all Class Members about the threats that they because of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves; and

xiii. Incidental retrospective relief, including but not limited to restitution.

VII. CAUSES OF ACTION

COUNT I: NEGLIGENCE/NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of the State Subclasses, against WebTPA)

418. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 417 above as if fully set forth herein.

419. Defendants required Plaintiffs and Class Members to submit, directly or indirectly, personal, confidential Private Information to WebTPA as a condition of receiving insurance coverage and related services.

420. Plaintiffs and Class Members, through Insurer Defendants, provided certain Private Information to WebTPA including their names, dates of birth, Social Security numbers, health information, and other sensitive information.

421. WebTPA had full knowledge of the sensitivity of the Private Information to which it was entrusted, and the types of harm that Plaintiff and Class Members could and would suffer if

the Private Information was wrongfully disclosed to unauthorized persons. WebTPA had duties to Plaintiffs and each Class Member to exercise reasonable care in holding, safeguarding, and protecting their Private Information.

422. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices by WebTPA.

423. Plaintiffs and Class Members had no ability to protect their Private Information in WebTPA's possession.

424. By collecting and storing Plaintiffs' and Class Members' Private Information, WebTPA had a duty of care to use reasonable means to secure and safeguard it, to prevent disclosure of the information, and to safeguard the Private Information from theft.

425. WebTPA's duty of care obligated it to implement processes by which it could detect if that Private Information was exposed to unauthorized actors, while Insurer Defendants' duty of care obligated them to ensure WebTPA's processes to detect compromises of Private Information were sufficient.

426. WebTPA owed a duty to Plaintiffs and Class Members to provide data security consistent with industry standards and legal and regulatory requirements, to ensure that its systems and networks and the personnel responsible for them adequately protected Plaintiffs' and Class Members' Private Information.

427. WebTPA was able to ensure that its systems and data security procedures were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a cybersecurity event like this Data Breach, whereas Plaintiffs and Class Members were not.

428. WebTPA had a duty to employ reasonable security measures 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 confidential data.

429. Pursuant to the FTC Act, WebTPA had a duty to provide adequate systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

430. WebTPA breached its duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information and by failing to encrypt or timely delete the Private Information from its network systems.

431. WebTPA's violations of the FTC Act as described herein directly caused and/or were a substantial factor in the Data Breach and resulting injuries to Plaintiffs and Class Members.

432. Plaintiffs and Class Members are within the class of persons the FTC Act was intended to protect.

433. The type of harm that resulted from the Data Breach was the type of harm the FTC Act was intended to guard against.

434. WebTPA's failures to comply with the FTC Act is negligence *per se.*

435. WebTPA's duties to use reasonable care in protecting Plaintiffs' and Class Members' Private Information arose not only as a result of the statutes and regulations described above, but because WebTPA is bound by industry standards to secure such Private Information.

436. WebTPA breached its duties and was negligent by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure in the Data Breach. The specific negligent acts and omissions committed by WebTPA include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard

Plaintiff's and Class Members' Private Information;

b. Failing to adequately train employees on proper cybersecurity protocols;

c. Failing to adequately monitor the security of its information technology networks and systems;

d. Failure to periodically ensure that its network systems had plans in place to maintain reasonable data security safeguards;

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

f. Failing to timely notify Plaintiffs and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

437. But for WebTPA's wrongful and negligent breaches of its duties owed to Plaintiffs and Class Members, the Data Breach would not have occurred or at least would have been mitigated, Plaintiffs' and Class Members' Private Information would not have been compromised, and Plaintiffs' and Class Members' injuries would have been avoided.

438. It was foreseeable that WebTPA's failures to use reasonable measures to protect Plaintiffs' and Class Members' Private Information would injure Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable to WebTPA given the known high frequency of cyber-attacks and data breaches in WebTPA's industry.

439. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' Private Information would cause them one or more types of injuries.

440. As a direct and proximate result of WebTPA's negligence, Plaintiffs and Class Members have suffered and will suffer injuries and damages, including but not limited to (a)

invasion of privacy; (b) lost or diminished value of their Private Information; (c) actual identity theft and fraud; (d) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (e) loss of benefit of their bargain; and (f) the continued and certainly increased risk to their Private Information, which remains (i) unencrypted and available for unauthorized third parties to access and abuse; and (ii) in WebTPA's possession and subject to further unauthorized disclosures so long as WebTPA fails to undertake appropriate and adequate measures to protect it.

441. As a direct and proximate result of WebTPA's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injuries and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

442. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT II: NEGLIGENCE/NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of the State Subclasses, against Insurer Defendants)

443. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 417 above as if fully set forth herein.

444. Insurer Defendants required Plaintiffs and Class Members to submit, directly or indirectly, personal, confidential Private Information to Insurer Defendants and their business associate/vendor WebTPA as a condition of receiving insurance coverage and related services.

445. Plaintiffs and Class Members provided certain Private Information to Insurer Defendants and, through Insurer Defendants, to WebTPA, including their names, dates of birth, Social Security numbers, health information, and other sensitive information.

446. Insurer Defendants had full knowledge of the sensitivity of the Private Information to which they were entrusted, and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed to unauthorized persons. Insurer Defendants had duties to Plaintiffs and each Class Member to exercise reasonable care in holding, safeguarding, and protecting their Private Information, including requiring and ensuring their business associate/vendors handling Private Information had reasonable and appropriate data security measures and policies in place to do so.

447. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices by Insurer Defendants or their business associate/vendor WebTPA.

448. Plaintiffs and Class Members had no ability to protect their Private Information in Insurer Defendants' or WebTPA's possession.

449. By collecting and storing Plaintiffs' and Class Members' Private Information, Insurer Defendants had a duty of care to use reasonable means to secure and safeguard it, to prevent disclosure of the information, and to safeguard the Private Information from theft.

450. Insurer Defendants' duty of care obligated them to require and ensure that WebTPA provided data security data security consistent with industry standards and legal and regulatory requirements, and that WebTPA's systems and networks and the personnel responsible for them adequately protected Plaintiffs' and Class Members' Private Information.

451. Insurer Defendants' duty of care further obligated them to ensure WebTPA's processes to detect compromises of Private Information were sufficient.

452. Insurer Defendants were able to ensure WebTPA's systems and data security procedures were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a cybersecurity event like this Data Breach, whereas Plaintiffs and Class Members

were not.

453. Insurer Defendants had a duty to employ reasonable security measures 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 confidential data.

454. Pursuant to the FTC Act, 15 U.S.C. § 45, Insurer Defendants had a duty to provide adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PHI.

455. Pursuant to HIPAA, 42 U.S.C. § 1302d *et seq*., Insurer Defendants had the further duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' PHI from unauthorized disclosure.

456. Pursuant to HIPAA, Insurer Defendants had a duty to require WebTPA implement reasonable data security measures for the PHI in its care, including by, *e.g.*, rendering the electronic PHI it maintained in a form unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* 45 C.F.R. § 164.304.

457. Additionally, pursuant to HIPAA, Insurer Defendants had a duty to provide notice of the Data Breach within 60 days of discovering it. *See* 42 C.F.R. § 2.16(b); 45 C.F.R. § 164.404(b).

458. Insurer Defendants breached their duties to Plaintiffs and Class Members under the FTC Act and HIPAA by failing to require their business associate/vendor WebTPA to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs'

and Class Members' Private Information, by failing to ensure the Private Information on WebTPA's system was encrypted and timely deleted when no longer needed, and by failing to provide notice to Plaintiffs and Class Members of the Data Breach until over 60 days after Insurer Defendants discovered it.

459. Insurer Defendants' violations of the FTC Act and HIPAA as described herein directly caused and/or were a substantial factor in the Data Breach and resulting injuries to Plaintiffs and Class Members.

460. Plaintiffs and Class Members are within the class of persons the FTC Act and HIPAA were intended to protect.

461. The type of harm that resulted from the Data Breach was the type of harm the FTC Act and HIPAA were intended to guard against.

462. Insurer Defendants' failures to comply with the FTC Act and HIPAA is negligence *per se.*

463. Insurer Defendants' duties to use reasonable care in protecting Plaintiffs' and Class Members' Private Information arose not only as a result of the statutes and regulations described above, but also because Insurer Defendants are bound by industry standards to secure such Private Information.

464. Insurer Defendants breached their duties and were negligent by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure in the Data Breach. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to require and periodically ensure that WebTPA adopted, implemented, and maintain adequate security measures to safeguard Plaintiff's and Class Members'

Private Information;

b. Failing to adequately monitor the security of WebTPA's information technology networks and systems;

c. Failure to require and periodically ensure that WebTPA's network systems had plans in place to maintain reasonable data security safeguards;

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

e. Failing to timely notify Plaintiffs and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

465. But for Insurer Defendants' wrongful and negligent breaches of their duties owed to Plaintiffs and Class Members, the Data Breach would not have occurred or at least would have been mitigated, Plaintiffs' and Class Members' Private Information would not have been compromised, and Plaintiffs' and Class Members' injuries would have been avoided.

466. It was foreseeable that Insurer Defendants' failures to use reasonable measures to protect Plaintiffs' and Class Members' Private Information would injure Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable to Insurer Defendants given the known high frequency of cyber-attacks and data breaches in Defendants' industry.

467. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' Private Information would cause them one or more types of injuries.

468. As a direct and proximate result of Insurer Defendants' negligence, Plaintiffs and Class Members have suffered and will suffer injuries and damages, including but not limited to (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) actual identity

theft and fraud; (d) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (e) loss of benefit of their bargain; and (f) the continued and certainly increased risk to their Private Information, which remains (i) unencrypted and available for unauthorized third parties to access and abuse; and (ii) in Insurer Defendants' and WebTPA's possession and subject to further unauthorized disclosures so long as Insurer Defendants and WebTPA fail to undertake appropriate and adequate measures to protect it.

469. As a direct and proximate result of Insurer Defendants' negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injuries and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

470. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III: BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of the State Subclasses, against Insurer Defendants)

471. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 417 above as if fully set forth herein.

472. Insurer Defendants required Plaintiffs and Class Members to provide and entrust their Private Information to Insurer Defendants as a condition of obtaining insurance products and related services.

473. When Plaintiffs and Class Members provided their Private Information to Insurer Defendants, they entered into implied contracts with Insurer Defendants pursuant to which Insurer Defendants agreed to safeguard and protect such Private Information and to timely and accurately

notify Plaintiffs and Class Members if and when their Private Information was breached and compromised.

474. Specifically, Plaintiffs and Class Members entered into valid and enforceable implied contracts with Insurer Defendants when they agreed to provide their Private Information and/or payment to Insurer Defendants.

475. The valid and enforceable implied contracts that Plaintiffs and Class Members entered into with Insurer Defendants included Insurer Defendants' promises to protect Private Information they collected from Plaintiffs and Class Members, or created on their own, from unauthorized disclosures. Plaintiffs and Class Members provided this Private Information in reliance on Insurer Defendants' promises.

476. Under the implied contracts, Insurer Defendants promised and were obligated to (a) provide insurance coverage and related services to Plaintiffs and Class Members; and (b) protect Plaintiffs' and Class Members' Private Information provided to obtain such services and/or created in connection therewith. In exchange, Plaintiffs and Class Members agreed to provide Insurer Defendants with payment and their Private Information.

477. Insurer Defendants promised and warranted to Plaintiffs and Class Members, including through their public-facing privacy documents identified above, to maintain the privacy and confidentiality of the Private Information they collected from Plaintiffs and Class Members and to keep such information safeguarded against unauthorized access and disclosure.

478. Insurer Defendants' adequate protection of Plaintiffs' and Class Members' Private Information was a material aspect of these implied contracts with Insurer Defendants.

479. Insurer Defendants solicited and invited Plaintiffs and Class Members to provide their Private Information as part of Insurer Defendants' regular business practices. Plaintiffs and

Class Members accepted Insurer Defendants' offers and provided their Private Information to Insurer Defendants.

480. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Insurer Defendants' data security practices complied with industry standards and relevant laws and regulations, including the FTC Act, HIPAA, HITECH, and industry standards.

481. Plaintiffs and Class Members who contracted with Insurer Defendants for insurance coverage and related services and provided their Private Information to Insurer Defendants reasonably believed and expected that Insurer Defendants would adequately employ adequate data security to protect that Private Information. Insurer Defendants failed to do so.

482. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their Private Information to Insurer Defendants and agreed Insurer Defendants would receive payment for, amongst other things, the protection of their Private Information.

483. Plaintiffs and Class Members performed their obligations under the contracts when they provided their Private Information and/or payment to Insurer Defendants.

484. Insurer Defendants materially breached their contractual obligations to protect the Private Information they required Plaintiffs and Class Members to provide when that Private Information was unauthorizedly disclosed in the Data Breach due to Insurer Defendants' inadequate data security measures and procedures.

485. Insurer Defendants materially breached their contractual obligations to deal in good faith with Plaintiffs and Class Members when they failed to take adequate precautions to prevent the Data Breach and failed to promptly notify Plaintiffs and Class Members of the Data Breach.

486. Insurer Defendants materially breached the terms of their implied contracts,

including but not limited to by failing to comply with industry standards or the standards of conduct embodied in statutes like Section 5 of the FTC Act, by failing to otherwise protect Plaintiffs' and Class Members' Private Information, and/or by failing to prevent the same data security failures by their business associate/vendor WebTPA that handled Private Information, as set forth *supra*.

487. The Data Breach was a reasonably foreseeable consequence of Insurer Defendants' conduct, by acts of omission or commission, in breach of these implied contracts with Plaintiffs and Class Members.

488. As a result of Insurer Defendants' failures to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive the full benefit of their bargains with Insurer Defendants, and instead received services of a diminished value compared to that described in the implied contracts. Plaintiffs and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

489. Had Insurer Defendants disclosed that their data security procedures were inadequate or that they did not adhere to industry-standard for cybersecurity, neither Plaintiffs, Class Members, nor any reasonable person would have contracted with Insurer Defendants.

490. Plaintiffs and Class Members would not have provided and entrusted their Private Information to Insurer Defendants in the absence of the implied contracts between them and Insurer Defendants.

491. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Insurer Defendants.

492. Insurer Defendants breached the implied contracts they made with Plaintiffs and Class Members by failing to safeguard and protect their Private Information and by failing to

provide timely or adequate notice that their Private Information was compromised in and due to the Data Breach.

493. As a direct and proximate result of Insurer Defendants' breach of their implied contracts with Plaintiffs and Class Members and the attendant Data Breach, Plaintiffs and Class Members have suffered injuries and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they struck with Insurer Defendants.

494. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or restitution, in an amount to be proven at trial.

495. Plaintiffs and Class Members are also entitled to injunctive relief requiring Insurer Defendants to, *e.g.*, (a) strengthen their data security systems and monitoring procedures; (b) conduct annual audits their vendor's data security systems and monitoring procedures; and (c) provide adequate lifetime credit monitoring to all Class Members.

COUNT IV: BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of the State Subclasses, against WebTPA)

496. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 417 above as if fully set forth herein.

497. WebTPA entered into uniform written contracts with its clients, including Insurer Defendants, to provide administrative and claims processing services.

498. Pursuant these contracts, WebTPA received from its clients and maintained Plaintiffs' and Class Members' Private Information in the course of providing administrative and claims processing services, which it could not perform without receiving and maintaining such Private Information.

499. Pursuant to these contracts, WebTPA's clients, including Insurer Defendants,

agreed to provide WebTPA with compensation and Plaintiffs' and Class Members' Private Information.

500. In exchange, WebTPA agreed, in part, to implement adequate data security measures to safeguard Plaintiffs' and Class Members' Private Information from unauthorized disclosure, and to timely notify Plaintiffs and Class Members of the Data Breach.

501. Insurer Defendants were required by statute and regulation, including but not limited to HIPAA and state consumer privacy and protection laws, to have contracts with WebTPA requiring WebTPA to implement and maintain reasonable security procedures and practices to protect Insurer Defendants' customers'—Plaintiffs and Class Members—Private Information from unauthorized access, use, or disclosure.

502. The relevant statutes and regulations obligating Insurer Defendants to require by contract that WebTPA use reasonable data security for Plaintiffs' and Class Members' Private Information create a class of intended beneficiaries whose members are implied into such agreements by operation of law. Plaintiffs and Class Members are the intended beneficiaries of the contracts that Insurer Defendants entered into with WebTPA to satisfy these statutory and regulatory requirements.

503. Upon information and belief, WebTPA's contracts with its clients, including Insurer Defendants, each contained a provision requiring WebTPA implement and maintain reasonable security procedures and practices appropriate to the nature of Private Information WebTPA collected, to protect the Private Information from unauthorized access, use, or disclosure.

504. These contracts between WebTPA and its clients, including Insurer Defendants, were made to facilitate the transactions between Insurer Defendants their customers, Plaintiffs and Class Members, and were made expressly for the benefit of Plaintiffs and Class Members as the

intended third-party beneficiaries of these contracts.

505. WebTPA knew Plaintiffs and Class Members were involved and would benefit from the transactions that were subject to these contracts between Insurer Defendants and WebTPA.

506. WebTPA knew that if it breached its contractual obligation to adequately safeguard its clients' customers' Private Information, Insurer Defendants' customers—Plaintiffs and Class Members—would be harmed.

507. WebTPA breached these contracts with Insurer Defendants, by, among other acts and omissions, (a) failing to use reasonable data security measures, (b) failing to implement adequate protocols and employe training sufficient to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure, and (b) failing to promptly or adequately notify Plaintiffs and Class Members of the Data Breach.

508. As a direct and proximate result of WebTPA's breaches of these contracts with Insurer Defendants, Plaintiffs and Class Members have suffered and will continue to suffer injuries as set forth herein, and are entitled to damages sufficient to compensate for the losses they sustained as a direct result thereof.

509. Plaintiffs are further entitled to recover against WebTPA Plaintiffs' costs and attorney's fees incurred in this action.

COUNT V: CALIFORNIA CONSUMER PRIVACY ACT
Ca. Civ. Code § 1798.100, *et seq.* ("CCPA")
(On Behalf of the California Subclass against WebTPA)

510. Plaintiffs Tracy Bertocchini and Mark Ellak (for purposes of this count, "Plaintiffs") re-allege and incorporate by reference paragraphs 1–250 and 402–17 above as if fully set forth herein.

511. At all relevant times, WebTPA has done business in the State of California.

512. The CCPA imposes a duty on entities doing business in the State of California to implement and maintain reasonably security procedures and practices as appropriate given the nature of the sensitive information.

513. Under the CCPA, a business's "collection, use, retention, and sharing of a consumer's personal information" shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes. Ca. Civ. Code § 1798.100(c).

514. Further, under the CCPA, "[a] business that collects a consumer's personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure." Ca. Civ. Code § 1798.100(e); *see also* § 1798.81.5.

515. Pursuant to the CCPA, any individual whose nonencrypted and nonredacted personal information is accessed, exfiltrated, stolen, or disclosed as a result of the business's violation of its duty to collect, use, retain, and share personal information about a consumer only in manners compatible with the business's purpose in collecting such information are entitled to damages, including statutory damages. Ca. Civ. Code § 1798.150.

516. Plaintiffs' and California Subclass Members' Private Information compromised in the Data Breach is "personal information about a consumer" as used in the CCPA. Ca. Civ. Code §§ 1798.80(e), 1798.150(a).

517. WebTPA collected Plaintiffs' and California Subclass Members' Private

Information for the purpose of providing administrative services to WebTPA's clients.

518. When the Data Breach occurred, WebTPA maintained Plaintiffs' and California Subclass Members' Private Information in unencrypted and unredacted form.

519. When the Data Breach occurred, WebTPA did not have reasonable security procedures and practices appropriate to the nature of the Private Information it collected to protect such Private Information from unauthorized or illegal access, destruction, use, or disclosure.

520. Exposure of Plaintiffs' and California Subclass Members' Private Information to unauthorized third-parties, as in this Data Breach, is incompatible with WebTPA's purpose in collecting or processing such information.

521. WebTPA violated the CCPA by failing to implement data security measures as reasonably necessary and proportionate to protect Plaintiffs' and California Subclass Members' Private Information it collected and processed.

522. WebTPA further violated the CCPA by failing to use Plaintiffs' and California Subclass Members' Private Information in a manner that is reasonably necessary and proportionate to achieve the purposes for which such Private Information was collected.

523. As a direct and proximate result of WebTPA's failure to implement reasonably necessary and proportionate data security measures as required by the CCPA, Plaintiffs' and California Subclass Members' unencrypted and unredacted Private Information was wrongfully disclosed to unauthorized cybercriminals in the Data Breach, causing Plaintiffs' and Class Members' injuries and damages as set forth herein.

524. On June 25, 2024, Plaintiff Ellak on behalf of himself and the California Subclass sent WebTPA notice of this CCPA claim, which WebTPA received on July 1, 2024. To date, WebTPA has failed to cure its CCPA violations.

525. Plaintiffs and the California Subclass are entitled to damages, including statutory damages, due to WebTPA's CCPA violations. Ca. Civ. Code § 1798.150.

COUNT VI: ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT 815 Ill. Comp. Stat. § 505/1, *et seq*. ("ICFA")
(On Behalf of the Illinois Subclass against WebTPA and Hartford)

526. Plaintiff Sofia Bersineva (for the purposes of this count, "Plaintiff") re-alleges and incorporates by reference paragraphs 1–224, 295–309, and 402–417 above as if fully set forth herein.

527. Plaintiff and the Illinois Subclass are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e).

528. Defendants WebTPA and Hartford (for purposes of this count, collectively, "Defendants"), Plaintiff, and Illinois Subclass Members are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

529. Defendants engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendants also engage in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

530. Pursuant to Defendants' trade or commerce, Defendants disclosed Plaintiff's and Illinois Subclass Members' Private Information to unauthorized parties in the Data Breach.

531. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the ICFA, including: (i) failing to maintain and/or ensure that adequate data security was used—including by WebTPA—as to keep Plaintiff's and Illinois Subclass Members' sensitive Private Information from being accessed or stolen by cybercriminals and failing to comply with applicable state and federal laws and industry

standards pertaining to data security, including the FTC Act; (ii) failing to disclose or omitting materials facts to Plaintiff and Illinois Subclass Members regarding the lack of adequate data security and inability or unwillingness to properly secure and protect the Private Information of Plaintiff and Illinois Subclass Members; (iii) failing to disclose or omitting materials facts to Plaintiff and Illinois Subclass Members about Defendants' failures to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Plaintiff's and Illinois Subclass Members' Private Information; and (iv) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff's and Illinois Subclass Members' Private Information from further unauthorized disclosure, release, data breaches, and theft.

532. These actions also constitute deceptive and unfair acts or practices because Defendants knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and Illinois Subclass Members and if known, would defeat their reasonable expectations regarding the security of their Private Information.

533. Defendants intended that Plaintiff and Illinois Subclass Members rely on their deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendants' offering of insurance products and services.

534. Defendants' wrongful practices were and are injurious to the public because those practices were part of Defendants' generalized course of conduct that applied to the Illinois Subclass. Plaintiff and Illinois Subclass Members have been adversely affected by Defendants' conduct and the public was and is at risk as a result thereof.

535. As a result of Defendants' wrongful conduct, Plaintiff and Illinois Subclass

Members were injured in that they never would have provided their Private Information to Defendants or used Defendants' services, directly or indirectly, had they known or been informed that Defendants failed to maintain and/or ensure sufficient security to keep their Private Information from being wrongfully accessed, taken, and misused by unauthorized parties.

536. As a direct and proximate result of Defendants' violations of the ICFA, Plaintiff and Illinois Subclass Members have suffered harm, including but not limited to (a) the lost or diminished value of their Private Information; (b) actual identity theft and fraud; (c) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of their bargain; (e) future costs in terms of time, effort, and money that will be expended for the remainder of their lives to prevent, detect, contest, and repair the impact of the Private Information compromised due to the Data Breach; and (f) the continued and certainly increased risk to their Private Information, which remains (i) unencrypted and available for unauthorized third parties to access and abuse; and (ii) in Defendants' possession and subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect it.

537. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Illinois Subclass seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendants' violations of the ICFA.

COUNT VII: MISSOURI CONSUMER PROTECTION LAW
MO Rev. Stat. §§ 407.020, 407.025 ("MCPL")
(On Behalf of the Missouri Subclass against WebTPA)

538. Plaintiff Kenneth Reagan (for purposes of this count, "Plaintiff") re-alleges and incorporates by reference paragraphs 1–224 and 388–417 above as if fully set forth herein.

539. WebTPA is a "person" within the meaning of the MCPL and, at all pertinent times,

was subject to the MCPL's requirements and proscriptions with respect to all of WebTPA's business and trade practices described herein.

540. WebTPA engaged in unfair and deceptive trade practices by creating a false expectation of privacy to Missouri consumers, including Plaintiff and Missouri Subclass Members, through representations and promises that their Private Information in WebTPA's custody will be kept safe through adequate and reasonable data security measures that comply with the FTC Act, HIPAA, and industry standards, while in reality WebTPA failed to take commercially reasonable steps to protect the Private Information entrusted to it.

541. WebTPA engaged in deceptive and unfair acts and practices, misrepresentations, and the concealment and omission of material facts in connection with the sale and advertisement of services in violation of the MCPL, including without limitation by the following:

a. Failing to maintain adequate data security to keep Plaintiff's and Missouri Subclass Members' Private Information from being accessed and taken by cybercriminals;

b. Failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act, HIPAA, and/or HITECH;

c. Failing to disclose and omitting materials facts to Plaintiff and Missouri Subclass Members regarding WebTPA's lack of adequate data security and inability or unwillingness to properly secure and protect Plaintiff's and Missouri Subclass Members' Private Information;

d. Failing to disclose and/or omitting materials facts to Plaintiff and Missouri Subclass Members about WebTPA's noncompliance with relevant federal and state laws on the privacy and security of their Private Information; and

e. Failing to take proper action following the Data Breach to enact adequate privacy and

security measures and protect Plaintiff's and Missouri Subclass Members' Private Information from further unauthorized disclosure, release, breaches, and theft.

542. These actions also constitute deceptive and unfair acts or practices because WebTPA knew the facts about its inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and Missouri Subclass Members, and would erase the false impression of adequate security for their Private Information if known.

543. WebTPA's unfair acts and practices and deceptive misrepresentations and omissions would cause any reasonable person to enter, directly or indirectly, into the transactions between Plaintiff and Missouri Subclass Members and WebTPA and provide their Private Information to WebTPA in the course of such transactions, as WebTPA's insufficient and inadequate processes and practices regarding data security were concealed and unknown to Plaintiff, Missouri Subclass Members, and Missouri consumers in general.

544. Plaintiff and Missouri Subclass Members acted as a reasonable consumer would in light of all the circumstances in entrusting their Private Information to WebTPA, as they had no reason to believe that WebTPA, a sophisticated business entity, would maintain the Private Information using insufficient and inadequate data security measures.

545. But for WebTPA's unfair acts and practices and deceptive misrepresentations and omissions, Plaintiff and Missouri Subclass Members would have known the truth about its inadequate data security measures and would not have provided their Private Information to WebTPA, directly or indirectly.

546. WebTPA's wrongful practices were and are injurious to the public because they were and are part of its generalized course of conduct that applied to the Missouri Subclass as a

whole. Plaintiff, Missouri Subclass Members, and the public have been adversely affected by WebTPA's conduct and the public was and is at risk as a result thereof.

547. WebTPA's unfair acts and practices and deceptive misrepresentations and omissions as described herein took place in and/or from Missouri.

548. Plaintiff and Missouri Subclass Members have suffered ascertainable losses as direct result of WebTPA's use of unconscionable acts or practices, and unfair or deceptive acts or practices prohibited by the MCPL.

549. As a direct and proximate result of WebTPA's violations of the MCPL, Plaintiff and Missouri Subclass Members have suffered and will suffer harm, including but not limited to lost or diminished value of their Private Information, actual identity theft and fraud, lost opportunity costs and lost time associated with attempting to mitigate the actual consequences of the Data Breach, loss of benefit of the bargain, and other harm resulting from the unauthorized use and/or threat of unauthorized use of their compromised Private Information, entitling them to damages in an amount to be proven at trial.

550. Under the MCPL, Plaintiff and Missouri Subclass Members are entitled to recover actual damages incurred due to WebTPA's MCPL violations.

551. Pursuant to the MCPL, Plaintiff and Missouri Subclass Members are further entitled, as appropriate, to an award of punitive damages, equitable/injunctive relief, and reasonable attorney's fees against WebTPA due to WebTPA's MCPL violations.

COUNT VIII: NEW YORK GENERAL BUSINESS LAW
N.Y. Gen. Bus. L. § 349 *et seq.* ("GBL")
(On Behalf of the New York Subclass against WebTPA and Hartford)

552. Plaintiff Leonard Finkel (for the purposes of this count, "Plaintiff") re-alleges and incorporates by reference paragraphs 1–224, 364–75, and 402–17 above as if fully set forth

herein.

553. Defendants WebTPA and Hartford (for purposes of this count, collectively, "Defendants") engaged in deceptive acts or practices in the conduct of their business, trade, and commerce or furnishing of services, in violation of the GBL, including without limitation through the following:

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

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass Members' Private Information, including duties imposed by the FTC Act, HIPAA, and HITECH, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and New York Subclass Members' Private Information, including by implementing and maintaining, and requiring their vendors to implement and maintain, reasonable data security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New York Subclass Members' Private Information, including duties imposed by the FTC Act, HIPAA, and HITECH;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or

adequately secure Plaintiff's and New York Subclass Members' Private Information; 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 Plaintiff's and New York Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164.

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

555. Defendants acted intentionally, knowingly, and maliciously to violate New York's GBL, and recklessly disregarded Plaintiff and New York Subclass Members' rights.

556. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiff and New York 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 and other accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendants' services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

557. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the residents of New York affected and harmed by the Data Breach.

558. Defendants' deceptive and unlawful practices and acts caused substantial injury to

Plaintiff and New York Subclass Members that they could not reasonably avoid.

559. Plaintiff and New York Subclass Members seek all monetary and non-monetary relief allowed under the GBL, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

COUNT IX: NORTH CAROLINA CONSUMER PROTECTION LAW
NC Gen. Stat. §§ 407.020, 407.025 ("NCCPL")
(On Behalf of the North Carolina Subclass against WebTPA and Hartford)

560. Plaintiff Heavenle Wood (for the purposes of this count, "Plaintiff") re-alleges and incorporates by reference paragraphs 1–224, 310–22, and 402–17 above as if fully set forth herein.

561. Defendants WebTPA and Hartford (for purposes of this count, collectively, "Defendants") engaged in deceptive acts or practices in or affecting commerce in violation of the NCCPL, including without limitation through the following:

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

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and North Carolina Subclass Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's

and North Carolina Subclass Members' Private Information, including by implementing and maintaining, and requiring their vendors to implement and maintain, reasonable data security measures;

e. Misrepresenting that they would comply with common law and statutory duties regarding the security and privacy of Plaintiff's and North Carolina Subclass Members' Private Information, including duties imposed by the FTC Act, HIPAA, and HITECH;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and North Carolina Subclass Members' Private Information; 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 Plaintiff's and North Carolina Subclass Members' Private Information, including duties imposed by the FTC Act, and HIPAA, and HITECH.

562. Defendants acted intentionally, knowingly, and maliciously to violate the NCCPL and recklessly disregarded Plaintiff and North Carolina Subclass Members' rights.

563. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff and North Carolina Subclass Members have suffered and will continue to suffer injuries, including but not limited to (a) the lost or diminished value of their Private Information; (b) actual identity theft and fraud; (c) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) loss of benefit of their bargain; (e) future costs in terms of time, effort, and money that will be expended for the remainder of their lives to prevent, detect, contest, and repair the impact of the Private Information compromised due to the Data Breach; (f) invasion of privacy; and (g)

emotional distress, anxiety, and stress due to their Private Information's exposure and the consequential risk of identity theft facing Plaintiff and North Carolina Subclass Members.

564. Plaintiff and North Carolina Subclass Members seek all relief provided under the NCCPL, including actual, compensatory, and treble damages.

COUNT X: PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW 73 P.S. § 201-1, *et seq.* ("UTPCPL")
(On Behalf of the Pennsylvania Subclass against WebTPA and Hartford)

565. Plaintiff Chanelle Zimmerman (for purposes of this count, "Plaintiff") re-alleges and incorporates by reference paragraphs 1–224, 350–63, and 402–17 as if fully set forth herein.

566. The UTPCPL prohibits unfair or deceptive acts or practices in trade or commerce, which prohibited acts or practices include, *inter alia*, representing that services have characteristics or benefits that they do not have, and representing that services are of a particular standard, quality or grade, if they are of another.

567. Defendants WebTPA and Hartford (for purposes of this count, collectively, "Defendants") engaged in trade or commerce as used in the UTPCPL because they advertised, sold, and distributed services and because Defendants' respective businesses directly or indirectly affected Pennsylvania residents.

568. Plaintiff, Pennsylvania Subclass Members, and Defendants are all "persons" as defined and used in the UTPCPL.

569. Plaintiffs and Pennsylvania purchased services, directly or indirectly, from Defendants for personal and/or family purposes.

570. Defendants engaged in unfair or deceptive acts and practices in trade or commerce that affected Pennsylvania residents, directly or indirectly, in violation of the UTPCPL, by representing that Defendants had implemented reasonable and adequate data security processes

and procedures to protect Plaintiff and Pennsylvania Subclass Members' Private Information, when in reality, Defendants' data security processes and procedures were deficient and left Plaintiff and Pennsylvania Subclass Members' Private Information vulnerable to the Data Breach.

571. Defendants further engaged in unfair or deceptive acts and practices in trade or commerce that affected Pennsylvania residents, directly or indirectly, in violation of the UTPCPL, by representing that Defendants had implemented data security processes and procedures that complied with the FTC Act, HIPAA, and industry standards to protect Plaintiff and Pennsylvania Subclass Members' Private Information, when in reality, Defendants' data security processes and procedures did not comply with the FTC Act, HIPAA, or industry standards and left Plaintiff and Pennsylvania Subclass Members' Private Information vulnerable to the Data Breach.

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

573. Defendants acted intentionally, knowingly, and maliciously to violate the UTPCPL, and recklessly disregarded Plaintiff and Pennsylvania Subclass Members' rights.

574. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices and violations of the UTPCPL, Plaintiff and Pennsylvania Subclass Members have suffered and will continue to suffer ascertainable losses of money or property, including but not limited to fraud and identity theft; time and expenses related to monitoring their accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendants' services; loss of the value of their Private Information; and the cost of identity protection services made necessary by the Data Breach.

575. Pursuant to the UTPCPL, Plaintiff and Pennsylvania Subclass Members are each

entitled to recover the greater of (a) their actual damages resulting from Defendants' UTPCPL violations or (b) statutory damages of $100.00.

576. Plaintiff and Pennsylvania further seek treble damages, attorney's fees, and costs, as appropriate, due to Defendants' UTPCPL violations.

COUNT XI: UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of the State Subclasses, against all Defendants)

577. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 417 above as if fully set forth herein.

578. This count is brought in the alternative to the breach of implied contract count and the breach of third-party beneficiary contract count above.

579. Plaintiffs and Class Members conferred a benefit on Defendants by way providing, directly or indirectly, payment and their Private Information to Defendants as part of Defendants' respective businesses.

580. Defendants required Plaintiffs' and Class Members' Private Information to conduct their respective businesses and generate revenue, which they could not do without collecting and maintaining Plaintiffs' and Class Members' Private Information.

581. The monies paid to Defendants included a premium for Defendants' cybersecurity obligations and were supposed to be used by Defendants, in part, to pay for the administrative and other costs of providing reasonable data security and protection for Plaintiffs' and Class Members' Private Information.

582. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident,

Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

583. Defendants failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiffs and Class Members, and as a result, Defendants were overpaid.

584. Under principles of equity and good conscience, Defendants should not be permitted to retain the money because they failed to provide adequate safeguards and security measures to protect Plaintiffs' and Class Members' Private Information, which Plaintiffs and Class Members paid for but did not receive.

585. Defendants wrongfully accepted and retained these benefits—payment and Plaintiffs' and Class Members' Private Information—and were enriched to the detriment of Plaintiffs and Class Members.

586. Defendants' enrichment at Plaintiff's and Class Members' expense is unjust.

587. As a result of Defendants' wrongful conduct and resulting unjust enrichment, Plaintiffs and Class Members are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendants, plus reasonable attorneys' fees and costs.

COUNT XII: DECLARATORY JUDGMENT
(On behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of the State Subclasses, against all Defendants)

588. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 417 above as if fully set forth herein.

589. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is

authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary supplemental relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

590. In the fallout of the Data Breach, a controversy has arisen about Defendants' duties to use reasonable data security for the Private Information they collect and maintain.

591. On information and belief, Defendants' actions were—and *still* are—inadequate and unreasonable. Plaintiffs and Class Members continue to suffer injuries from the ongoing threat of fraud and identity theft due to Defendants' inadequate data security measures.

592. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring as follows:

a. Defendants owed—and continue to owe—a legal duty to use reasonable data security to secure the Private Information entrusted to them;

b. Defendants have a duty to notify impacted individuals of the Data Breach under the common law, Section 5 of the FTC Act, and HIPAA;

c. Defendants breached, and continue to breach, their duties by failing to use reasonable measures to protect the Private Information entrusted to them from unauthorized access, use, and disclosure; and

d. Defendants' breaches of their duties caused—and continues to cause—injuries to Plaintiffs and Class Members.

593. The Court should also issue injunctive relief requiring Defendants to use adequate security consistent with industry standards to protect the Private Information entrusted to them.

594. That Anthem was previously the target of one of the largest data breaches then-known, yet still refused to act proactively to prevent the exposure of millions of individuals'

Private Information in this Data Breach through improved data security measures, like thorough due diligence and oversight of its vendors handling Private Information, highlights the need for an injunction here—lest Defendants continue to skimp on cybersecurity to augment their own profits while leaving individuals like Plaintiffs and Class Members to suffer the consequences.

595. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injuries and lack an adequate legal remedy if Defendants experience a second data breach. And if a second breach occurs, Plaintiffs and Class Members will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full, and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted for out-of-pocket damages and other legally quantifiable and provable damages, cannot cover the full extent of Plaintiffs' and Class Members' injuries.

596. If an injunction is not issued, the resulting hardship to Plaintiffs and Class Members far exceeds the minimal hardship that Defendants could experience if an injunction is issued.

597. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiffs, Class Members, and the public at large.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for judgment as follows:

A. An Order certifying this case as a class action on behalf of Plaintiffs and the proposed Classes, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Classes;

B. Awarding Plaintiffs and the Classes damages that include applicable compensatory, actual, statutory, nominal, exemplary, and punitive damages, as allowed by law;

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

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

E. Awarding injunctive relief in the form of additional technical and administrative cybersecurity controls as is necessary to protect the interests of Plaintiffs and the Classes;

F. Enjoining Defendants from further deceptive practices and making untrue statements about their data security, the Data Breach, and the transmitted Private Information;

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

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

I. Awarding such further relief to which Plaintiffs and the Classes are entitled.

IX. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues to triable.

Dated: August 28, 2024

Respectfully submitted,

/s/ Jeff Ostrow
Jeff Ostrow (admitted *pro hac vice*)
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd, Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100
Fax: (954) 525-4300
ostrow@kolawyers.com

Gary Klinger (admitted *pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: 866-252-0878
Fax: 865-522-0049
gklinger@milberg.com

Interim Co-Lead Counsel for Plaintiffs and the Putative Class

Joe Kendall
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Tel: 214-744-3000
Fax: 214-744-3015
jkendall@kendalllawgroup.com

Liaison Counsel for Plaintiffs and the Putative Class

ClassAction.org
