IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
DAYTON DIVISION

ANDREW GIBSON, NAKIA KING, MARCIE STRICKLAND individually and on behalf of all others similarly situated, *Plaintiffs,* v. ONETOUCHPOINT WEST CORP., CARESOURCE, CARESOURCE OHIO, INC., CARESOURCE INDIANA, INC., and CARESOURCE GEORGIA, CO. *Defendants*.	)	Case No. Jury Trial Demanded

CLASS ACTION COMPLAINT

Plaintiffs, Andrew Gibson, Nakia King, and Marcie Strickland, individually and on behalf of the Class defined below of similarly situated persons, allege the following against OneTouchPoint West Corp., ("OTP"), Caresource, Caresource Ohio, Inc., Caresource Indiana, Inc., and Caresource Georgia, Co. (collectively "Caresource") based upon personal knowledge and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

INTRODUCTION

1. This class action arises out of the recent data breach on OTP's network that occurred on April 27, 2022 ("Data Breach"). As a result of the Data Breach, Plaintiffs, who were notified that their information was breached by an unauthorized party, and similarly situated individuals, suffered irreparable damage when their sensitive personal and protected health information was compromised and unlawfully accessed.

2. OTP admits that it was unable to determine what specific files the unauthorized actor viewed within the OTP network and because the impacted systems contained certain information related to individuals provided by its customers the company was unable to say definitively what personal information was accessed by the unauthorized actor.[1] Nevertheless, the information compromised in the Data Breach is believed to have included highly sensitive data that represents a gold mine for data thieves. This includes current and former patient **names, address, age, gender, member ID, health insurance plan name and health condition, and information provided during a health assessment** (collectively the "Private Information") provided by Caresource and other healthcare insurance companies that contract with OTP for marketing services. Additionally, Plaintiffs understand that for at least some customers of Caresource, the Social Security number was included in the compromised information.

3. The compromised information includes personally identifiable information ("PII"), which according to the United States General Services Administration, refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, and includes name, address and date of birth, among other identifiers.

4. Compromised information also includes protected health information ("PHI"), which is a subset of PII, and is defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1320d *et seq.,* as health information that can be tied to an individual through one or more of 18 identifiers, including name, geographical identifiers smaller than a state, medical record numbers, account numbers, and health insurance beneficiary numbers.

5. OTP learned about the data breach on April 28, 2022. On July 27, 2022, OTP confirmed that the company experienced a data breach, but did not notify the Plaintiffs until August 10, 2022 that they had been affected, over three months after discovering the breach. Despite this delay, the notification letter sent by OTP did not offer to change the Plaintiffs' Member ID or

[1] *Notice of Data Security Event,* OneTouchPoint, *available at* https://1touchpoint.com/notice-of-data-event (last visited August 24, 2022).

recommend protective measures aside from recommending that Plaintiffs "review your mail from CareSource to make sure it looks right."

6. Armed with the Private Information accessed in the Data Breach, and a three month head start, data thieves can commit a variety of crimes including, e.g., using Class Members' names and insurance information to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits.

7. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts and healthcare plans to guard against identity theft, including medical identity theft. Plaintiffs and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft. Plaintiffs and Class Members may also incur out of pocket costs for changing healthcare plan member information and monitoring medical documentation to protect themselves against medical identity theft.

8. Therefore, Plaintiffs and Class Members will show that they have suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

9. As a vendor for at least thirty-six health insurance carriers, including Caresource, OTP knew or should have known of the dangers of a data breach that could impact hundreds of thousands of consumers and the importance of protecting Private Information.

10. Plaintiffs bring this class action lawsuit to address Defendants' inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and Class Members that their information had been subject to the unauthorized access and precisely what specific type of information was accessed.

11. The potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to OTP and Caresource, who were on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

12. Plaintiffs' and Class Members' identities are now at risk because of Defendants' negligent conduct since the Private Information that OTP collected and maintained, provided by Caresource and other healthcare insurance entities, is now likely in the hands of data thieves and unauthorized third-parties.

13. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

14. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to OTP's data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

PARTIES

15. Plaintiff Andrew Gibson is, and at all times mentioned herein was, an individual citizen of the State of Indiana residing in the City of Greenwood in Johnson County.

16. Plaintiff Nakia King is, and at all times mentioned herein was, an individual citizen of the State of Ohio residing in the City of Akron in Summit County.

17. Plaintiff Marcie Strickland is, and at all times mentioned herein was, an individual citizen of the State of Georgia residing in the City of Milledgeville in Baldwin County.

18. OneTouchPoint West Corp. is a vendor that provides marketing solutions with its principal place of business at 1225 Walnut Ridge Drive, Hartland, Wisconsin 53029.

19. Caresource is a healthcare insurance entity and non-profit organization that provides healthcare insurance to over 2 million individuals in five states and has a principal place of business at 230 N. Main Street, Dayton, Ohio 45402.

20. Caresource Ohio, Inc. is a healthcare insurance entity and non-profit organization incorporated in Ohio that provides healthcare insurance, and has a principal place of business at 230 N. Main Street, Dayton, Ohio 45402.

21. Caresource Indiana, Inc. is a healthcare insurance entity and non-profit organization incorporated in Indiana and has a principal place of business at 135 N. Pennsylvania Street, Suite 1300, Indianapolis, IN 46204.

22. Caresource Georgia, Co. is a healthcare insurance entity and non-profit organization incorporated in Georgia and has a principal place of business at 600 Galleria Parkway, Suite 400, Atlanta, GA, 30339.

JURISDICTION AND VENUE

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

24. This Court has personal jurisdiction over Defendants because Defendants transact business within the State of Ohio and committed one or more tortious acts in this District.

25. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Defendants have caused harm to Class Members residing in this District. Additionally, the Caresource headquarters is located within the District.

RELEVANT FACTUAL ALLEGATIONS

Caresource Healthcare Insurance

26. Plaintiffs and Class Members purchased healthcare insurance policies from Caresource, entered into contracts with Caresource when they applied and paid for insurance and Caresource issued them a policy.

27. Consideration for services provided by Caresource pursuant to individual contracts is the payment of premiums by Plaintiffs and Class Members to Caresource.

28. In the ordinary course of obtaining healthcare insurance, customers are required to provide sensitive personal and private information such as:

- Names;
- Addresses,
- Dates of birth;
- Gender;
- Social Security numbers;
- Medical histories including health conditions; and
- Other sensitive health information provided during a healthcare insurance health assessment.

Plaintiffs and Class Members provided this information to Caresource to obtain healthcare insurance coverage.

29. The Caresource website refers to vendor responsibilities to comply with HIPAA and the Health Information Technology for Economic and Clinical Health ("HITECH") Act, 42 U.S.C. § 300jj *et seq.;* § 17901 *et seq.* Under HITECH Act, HIPAA covered entities must promptly notify affected individuals of breaches of PHI, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals. Under HITECH Act, OTP must notify Caresource of breaches by OTP.

30. The Caresource Code of Conduct stresses the mitigation of risk and states that "[i]ntegrity-based decision making and behaving ethically builds trust and confidence with our members, providers and regulators."[2]

[2] *Code of Conduct,* Caresource, *available at* https://www.caresource.com/documents/code-of-conduct/ (last visited September 18, 2022).

31. Caresource states in its privacy practices that it is responsible for protecting members' health information and further states Caresource is required by law to maintain the privacy and security of members' protected health information.[3]

32. It was objectively reasonable for Plaintiffs and Class Members to understand their contracts with Caresource to include the privacy policies of Caresource and its vendors. In addition,, all of the individual policy contracts Plaintiffs and Class Members entered into with Caresource incorporated Caresource's promise to comply with laws and regulations pertaining to the confidentiality of Private Information.

OneTouchPoint and Caresource

33. Caresource is responsible for ensuring that any third-party vendors it contracts with will safeguard the Private Information of its customers.

34. A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information, and is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.[4]

35. On information and belief, Caresource entered into a business associate agreement, or business associate contract, with OTP. Plaintiffs and Class Members are intended beneficiaries of the contract between Caresource and OTP, including specifically the contract terms pertaining to the confidentiality of policyholder information, including but not limited to HIPAA.

36. OTP offers marketing solutions to companies, primarily in the health care industry, offering full brand control, on-demand marketing execution, order management and local digital marketing. Specifically, OTP offers brand management, local marketing, print-pack-ship services, digital marketing, targeted direct mail, and managed services.

---

[3] *Privacy Practices,* Caresource, *available at* https://www.caresource.com/about-us/legal/hipaa-privacy-practices/hipaa-privacy-practices-ohio-medicaid/ (last visited September 18, 2022).

[4] *Business Associate Contracts*, U.S. Department of Health and Human Services (January 25, 2013), *available at* https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

37. OTP is a vendor for at least thirty-six healthcare insurance entities, including Caresource, providing services such as print-on-demand, secure communications, and a single sign-on storefront to manage enrollment materials for health plans, administrators and external partners.

38. OTP's website states it has helped insurers across the country recruit more members during the selling season and all year long for New-to-Medicare and Medicaid prospects.

39. OTP's website states that it is part of an exclusive group of organizations worldwide certified by the Health Information Trust Alliance ("HITRUST"). OTP claims that the security framework ensures solutions are built within secure web-based technology and is HIPAA compliant.

40. In providing marketing solutions to healthcare insurance entities, OTP made assurances that it would comply with HIPAA and protect Private Information provided by healthcare insurance entities. According to the OTP website, OTP locks down content to ensure forms and collateral remain compliant with state and federal regulations across locations and executes HIPAA compliant patient communication and marketing campaigns.[5]

41. As part of its normal operations, OTP frequently obtains and stores PII and PHI of individuals who are policyholders of healthcare insurance entities that contract with OTP for marketing services, including Caresource.

42. On information and belief, OTP uses centralized servers to store data provided by healthcare insurance entities, including customer PII and PHI.

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

[5] *Bringing Brands to Life,* OneTouchPoint, *available at* https://1touchpoint.com/services (last visited August 24, 2022).

44. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

45. Plaintiff and the Class Members relied on OTP and Caresource to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

46. Plaintiffs and Class Members would not have paid premiums to Caresource for healthcare insurance benefits had Caresource disclosed that they did not have procedures to ensure its vendors had adequate safeguards, procedures, and systems to reasonably protect their Private Information.

Data Breaches In Healthcare

47. According to the Ponemon Institute and Verizon Data Breach Investigations Report, the health industry experiences more data breaches than any other sector.[6] Regular PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[7] However, PHI can sell for as much as $363 according to the Infosec Institute.[8] This is because one's personal health history, can't be changed, unlike credit card information.

48. PHI has increased value 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 also be used to create fake insurance claims, allowing for the purchase and resale of medical equipment. Some criminals use PHI to illegally gain access to prescriptions for their own use or resale.

Data Breach

49. According to OTP, on April 28, 2022, it discovered encrypted files on certain computer systems. OTP launched an investigation to determine the nature and scope of the cyberattack. As a result of the investigation, OTP determined that there was unauthorized access

---

[6] *Data Breaches: In the Healthcare Sector*, Center for Internet Security, *available at* https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited August 10, 2022).
[7] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (October 16, 2019), *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.
[8] *Data Breaches: In the Healthcare Sector*, Center for Internet Security, *available at* https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited August 10, 2022).

to certain OTP servers beginning on April 27, 2022. On June 1, 2022, OTP learned that it would be unable to determine what specific files the unauthorized actor viewed within the its network. OTP provided a summary of the investigation to its corporate clients, including Caresource, beginning on June 3, 2022.

50. OTP claims it began notifying affected individuals on July 27, 2022, however, Plaintiffs received notification letters dated August 10, 2022, more than three months following the discovery of the suspicious activity.

51. On information and belief, for all individuals affected, the compromised data includes member name, address, age, gender, member id, health condition and plan name, and for a subset of individuals affected, the data also included vital signs, medications, allergies, health screenings, and immunizations. However, on information and belief, Caresource has not notified the individuals who belong to the subset of individuals who have had additional PHI compromised.

52. This compromised PII and PHI can and likely will be sold either on the dark web or by other nefarious actors.

53. Defendants had obligations created by HIPAA, contract, industry standards, common law, and representations made directly or indirectly to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

54. OTP had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties.

55. Caresource had a duty to ensure that its vendors, including OTP, adopted reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosures to third parties.

56. Plaintiff and Class Members provided their Private Information through Caresource to OTP with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of security breaches.

57. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

58. Defendants knew or should have known that OTP's electronic records would be targeted by cybercriminals.

59. On information and belief, OTP failed to implement sufficient measures to prevent cyberattacks and Caresource failed to ensure that OTP had implemented sufficient measures to safeguard Plaintiffs' and Class Members' Private Information.

60. OTP could have prevented, but on information and belief they failed to prevent, this Data Breach by properly securing and encrypting the systems containing Plaintiffs' and Class Members' Private Information. Caresource could have ensured, but on information and belief they failed to ensure, that OTP properly secured and encrypted the Private Information on its systems prior to providing Plaintiffs' and Class Members' Private Information to OTP.

61. OTP and Caresource were negligent by ignoring repeated warnings and alerts directed to companies that store Private Information, including PHI, to protect and secure the sensitive data they possess.

62. Despite the prevalence of public announcements of data breaches targeting entities that store PHI, Defendants failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

Notice to Plaintiffs

Plaintiff Nakia King

63. With the exception of a two-month period in early 2020, for the past eighteen years Plaintiff Ms. King has held healthcare insurance through CareSource, a customer of OTP for print and mail fulfillment services.

64. Plaintiff Ms. King and her minor child are on the same healthcare insurance plan through CareSource.

65. As a mandatory part of maintaining healthcare insurance with CareSource, Ms. King provided PII, medical history and sensitive private health information for herself and her minor child to CareSource.

66. On information and belief, CareSource provided the Private Information of Ms. King and her minor child, including PII and PHI to OTP.

67. OTP created and maintained records that contained sensitive health information regarding Ms. King.

68. Ms. King received a letter from OTP, dated August 10, 2022, with the subject "Notice of Security Breach." This letter informed her that her data may have been compromised by the data security incident discovered on April 28, 2022. Nevertheless, OTP's notice letter to Ms. King stated that OTP "cannot be sure" whether Ms. King's information was viewed or removed from the OTP systems. Instead, it states only that the information impacted includes Ms. King's name, address, age, gender, member ID, health condition and plan name.

69. The notice letter from OTP contains a recommendation that Ms. King "should always review [her] mail from CareSource to make sure it looks right." However, other than providing a call center number that victims could contact with "any questions," OTP offered no other substantive steps to help victims like Plaintiff and the Class Members to protect themselves.

70. On information and belief, OTP sent a similar generic letter to all individuals affected.

71. Ms. King has received additional scam phone calls and email since the Data Breach, including emails referencing her health condition and regarding medications she takes. Ms. King believes that the increased scam calls and emails are a direct result of the OTP breach.

72. Plaintiff Ms. King is suffering from substantial increased anxiety and mental anguish. Beyond the normal risks presented by a data breach, Ms. King is concerned about the increased risk that her family, friends and associates will learn about her confidential and sensitive medical history, including but not limited to her health condition that was provided to OTP by Caresource.

Plaintiff Andrew Gibson

73. For the past several years, Plaintiff Mr. Gibson obtained healthcare insurance through CareSource.

74. As a mandatory part of the new patient intake with CareSource, Mr. Gibson provided his PII, medical history and sensitive private health information to CareSource.

75. On information and belief, CareSource provided the Private Information of Mr. Gibson, including his PII and PHI to OTP.

76. OTP created and maintained records that contained sensitive health information regarding Mr. Gibson.

77. Mr. Gibson received a letter from OTP, dated August 10, 2022, that was similar to the one Ms. King received. It had the subject "Notice of Security Breach" and informed him that his data may have been compromised by the data security incident discovered on April 28, 2022. Nevertheless, OTP's notice letter to Mr. Gibson stated that OTP "cannot be sure" whether Mr. Gibson's information was viewed or removed from the OTP systems. Instead, it states only that the information impacted includes Mr. Gibson's name, address, age, gender, member ID, health condition and plan name. However, as noted above, CareSource's public notice asserted that far more data was impacted than the OTP letter indicates.

78. Again, the OTP notice letter contains a recommendation that Mr. Gibson "should always review [his] mail from CareSource to make sure it looks right." Likewise, OTP offered no other substantive steps to help victims to protect themselves.

79. Mr. Gibson has received additional scam phone calls since the Data Breach and believes that the increased scam calls are a direct result of the OTP breach.

80. Plaintiff Mr. Gibson is suffering from substantial increased anxiety and mental anguish. Beyond the normal risks presented by a data breach, Mr. Gibson is concerned about the increased risk that his family, friends and associates will learn about his confidential and sensitive medical history, including but not limited to his health condition that was provided to OTP by Caresource.

Plaintiff Marcie Strickland

81. Starting from in or about August 2018 to the present, Plaintiff Ms. Strickland obtained healthcare insurance through CareSource.

82. As a mandatory part of the new patient intake for herself and her family with CareSource, Ms. Strickland provided PII, medical history and sensitive private health information regarding herself and her three minor children to CareSource.

83. On information and belief, CareSource provided the Private Information of Ms. Strickland and her minor children, including their PII and PHI to OTP.

84. OTP created and maintained records that contained sensitive health information regarding Ms. Strickland and her minor children.

85. Ms. Strickland received a letter from OTP, dated August 10, 2022, which again was similar to the letters received by Ms. King and Mr. Gibson. The letter had the subject "Notice of Security Breach." This letter informed her that her data may have been compromised by the data security incident discovered on April 28, 2022. As with the other plaintiffs, OTP's notice letter to Ms. Strickland stated that OTP "cannot be sure" whether Ms. Strickland's information was viewed or removed from the OTP systems. Instead, it states only that the information impacted includes the name, address, age, gender, member ID, health condition and plan name for Ms. Strickland and her children. Nevertheless, again, CareSource's public notice claimed that far more data was impacted than the OTP letter indicates.

86. The OTP notice letter then contained the same generic recommendation that Ms. Strickland "should always review your mail from CareSource to make sure it looks right," and it offered no other substantive steps to help victims to protect themselves.

87. Ms. Strickland has been forced to change her phone number due to spam phone calls she has received; and she has received an increased amount of spam emails to the email account that is connected with her Caresource account.

Defendants Failed To Comply With FTC Guidelines

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

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

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

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

92. On information and belief, OTP failed to properly implement basic data security practices. OTP's failure to employ reasonable and appropriate measures to protect against

unauthorized access to patient PII and PHI, and Caresource's failure to ensure OTP employed reasonable measures to safeguard the Private Information Caresource provided to OTP, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

93. Defendants were at all times fully aware of the obligation to protect the PII and PHI of Plaintiffs and Class Members they were entrusted with. Defendants knew or should have known of the significant repercussions that would result from its failure to do so.

Defendants Failed To Comply With Industry Standards

94. Experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

95. Several best practices have been identified that a minimum should be implemented by entities that obtain and store private health information, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

96. A number of industry and national best practices have been published and should be used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security ("CIS") released its Critical Security Controls, and all healthcare institutions are strongly advised to follow these actions.[9] The CIS Benchmarks are the only consensus-based, best-practice security configuration guides both developed and accepted by government, business, industry, and academia.[10]

97. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such

[9] *Data Breaches: In the Healthcare Sector*, Center for Internet Security, *available at* https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited August 10, 2022).
[10] *CIS Benchmarks FAQ*, Center for Internet Security, *available at* https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq (last visited August 10, 2022).

as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

98. On information and belief, OTP failed to meet the minimum standards of the following frameworks: the National Institute of Standards and Technology ("NIST") Cybersecurity Framework, the HIPAA Security Rule and Breach Notification Rule, the CIS Critical Security Controls, the Control Objectives for Information Related Technology ("COBIT"), ISO/IEC 27001, and HITRUST Common Security Framework, which are all established standards in reasonable cybersecurity readiness.

99. On information and belief, Caresource failed to ensure that OTP met the minimum standards of cybersecurity frameworks.

Defendants' Practices Violate HIPAA

100. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

101. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

102. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendants permitted to be compromised and/or stolen. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

103. As a business associate of Caresource, OTP was responsible for ensuring the confidentiality, integrity and availability of PHI in its possession. On information and belief,

OTP's Data Breach resulted from a combination of insufficiencies that demonstrate they failed to comply with safeguards mandated by HIPAA regulations.

104. Caresource had a business associate agreement, or business associate contract, with OTP that required OTP to comply with HIPAA related to uses of PHI. Specifically, to comply with HIPAA, the agreement should:

a. Stipulate that OTP will not use or further disclose the information other than as permitted by the contract or as required by law;
b. Require OTP to implement appropriate safeguards to prevent unauthorized uses or disclosures of the PHI;
c. Require OTP to report any use or disclosure not provided for by the agreement, including breaches of unsecured PHI;
d. Require OTP to satisfy individuals' requests for copies of PHI, incorporate any amendments, and account for the disclosure;
e. Require OTP to make available to HHS records relating to the use and disclosure of PHI in the event of an audit or investigation;
f. Require OTP to return or destroy PHI received from, created for, or received on behalf of, Caresource at the termination of the agreement;
g. Require OTP to ensure that any with access to PHI agree to the same restrictions and conditions that apply to Caresource; and
h. Authorize termination of the contract by Caresource if OTP violates any term of the agreement.

105. Caresource was required to ensure that all business associates, including OTP, were in compliance with HIPAA. On information and belief, Caresource failed to ensure that OTP was in compliance with safeguards mandated by HIPAA regulations. At a minimum, Caresource should have implemented the following measures to ensure Plaintiffs' and Class Members' PHI was safeguarded:

a. Conduct an accurate and thorough risk and vulnerability assessment of Caresource and OTP procedures to safeguard PHI in accordance with HIPAA;

b. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with HIPAA;

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

d. Obtain satisfactory assurances that OTP would properly safeguard PHI provided by Caresource in accordance with HIPAA;

e. Perform a periodic evaluation of OTP security policies and procedures to meet HIPAA requirements; and

f. Maintain records of periodic assessments of OTP policies and procedures to comply with HIPAA.

106. On information and belief, Caresource failed to exercise due diligence to ensure OTP was in compliance with HIPAA.

107. Caresource is not absolved of its obligations to obtain satisfactory assurances by entering into a business associate agreement with OTP.

OTP's Security Breach

108. On information and belief, CareSource and OTP entered into a valid business associate agreement requiring OTP to safeguard PHI in accordance with HIPAA. On information and belief, Plaintiffs and Class Members are third party beneficiaries of that agreement.

109. OTP breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. OTP's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

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

b. Failing to adequately protect Plaintiffs' and Class Members' Private Information;

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

d. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

e. Failing to properly implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to sufficiently implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

g. Failing to adequately implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

h. Failing to properly protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

i. Failing to properly protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

k. Failing to adequately train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

l. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI 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" (45 CFR § 164.304's definition of "encryption");

m. Failing to fully comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

n. Failing to adhere to industry standards for cybersecurity.

110. As the result of computer systems in need of security upgrading, inadequate procedures for handling emails containing viruses or other malignant computer code, and employees who opened files containing the virus or malignant code that perpetrated the cyberattack, OTP negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

111. Caresource negligently and unlawfully failed to ensure that OTP had implemented policies and procedures to safeguard Plaintiffs' and Class Members' Private Information.

112. Accordingly, as outlined below, Plaintiffs' and Class Members' daily lives were severely disrupted. What's more, they now face an increased risk of fraud and identity theft, including medical identity theft.

Healthcare Data Breaches, Fraud and Identity Theft

113. Cyberattacks are considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule: A breach under the HIPAA Rules is defined as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40.10.

114. The FTC hosted a workshop to discuss "informational injuries" which are injuries that consumers suffer from privacy and security incidents, such as data breaches or unauthorized disclosure of data.[11] Exposure of personal information that a consumer wishes to keep private, such as sensitive medical information, sexual orientation, or gender identity, may cause both market and non-market harm to the consumer, such as the ability to obtain or keep employment and negative impact on consumer's relationships with family, friends and coworkers. Healthcare data breaches can erode patients' trust in the ability of providers to protect their data, and may be less willing to seek treatment. Consumers loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

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

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

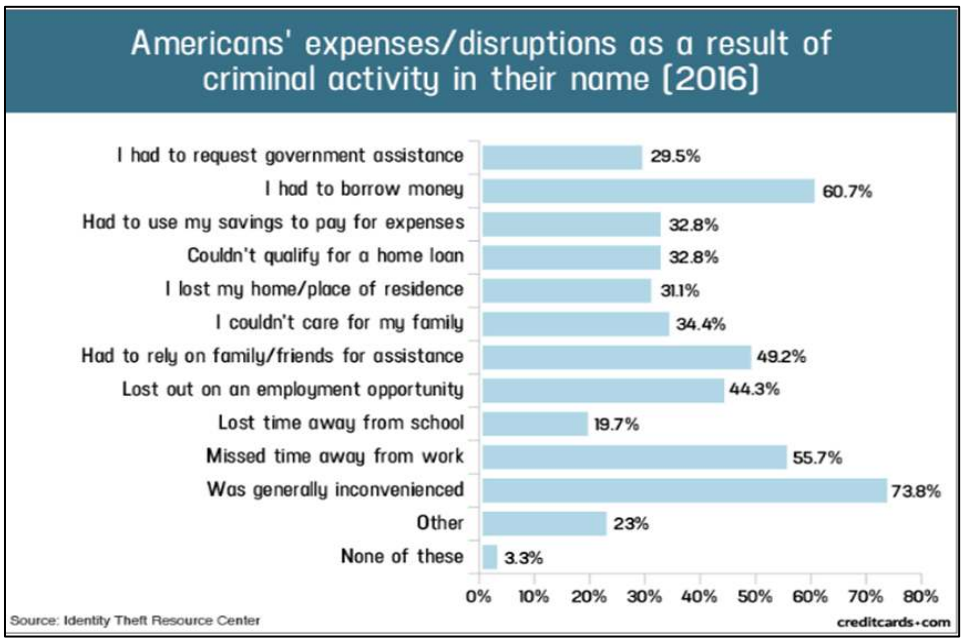
engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or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

116. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[12]

117. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of PII:[13]

[12] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited August 11, 2022).

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



118. Moreover, theft of Private Information is also gravely serious. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

119. Theft of PHI is gravely serious and can result in medical identity theft, where a thief uses the victim's information to see a doctor, get prescription drugs, buy medical devices, submit insurance claims, or get other medical care.[14] If the thief's health information is mixed with the victim's health information, it can negatively impact the victim's health insurance benefits and credit.

120. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

[14] *What To Know About Medical Identity Theft*, Federal Trade Commission (May 2021), *available at* https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

121. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[15]

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

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

123. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

124. Because of its value, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. As a vendor for at least thirty-six healthcare insurance entities, Defendants were entrusted with the Private Information of ten of thousands of individuals and knew or should have known of the threat of cyberattack and taken proactive steps to protect Private Information in its possession accordingly.

Defendants Owed A Duty to Plaintiffs' And Class Members'

125. Defendants owed a duty to Plaintiffs and Class Members to provide reasonable security including consistency with industry standards and requirements, and to ensure that their

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

computer systems and networks, and the personnel responsible for them, adequately protected the Private Information of Plaintiffs and Class Members. Caresource owed a duty to Plaintiffs and Class Members to ensure its vendors, including OTP, adequately protected the Private Information of Plaintiffs and Class Members it provided to OTP.

126. Defendants owed a duty to Plaintiffs and Class Members, who entrusted them with sensitive Private Information, to implement processes, and ensure its vendors implemented processes, that would detect a breach of their data security systems in a timely manner.

127. Defendants owed a duty to Plaintiffs and Class Members, who entrusted them with sensitive Private Information, to act upon data security warnings and alerts in a timely fashion and ensure its vendors did same.

128. Defendants owed a duty to Plaintiffs and Class Members, who entrusted them with sensitive Private Information, to disclose if their computer systems and data security practices, or those of its vendors, were inadequate to safeguard individuals' Private Information from theft. The disclosure of such an inadequacy would be a material fact in the decision to purchase insurance or other health care services from Caresource, or to entrust Private Information with Defendants.

129. Defendants owed a duty to Plaintiffs and Class Members, who entrusted them with sensitive Private Information, to disclose in a timely and accurate manner when data breaches occurred, and to ensure its vendors did same.

130. Defendants owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices by Defendants.

131. OTP collected Plaintiffs' and Class Members' Private Information either directly or indirectly from Caresource. Defendants knew that a breach of its data systems, or the data systems of its vendors, would cause Plaintiffs and Class Members to incur damages.

Caresource Breach of Contract

132. All of the contracts for healthcare insurance between Plaintiffs and Class Members and Caresource, as well as the contract between Caresource and OTP for which Plaintiffs and Class Members are intended beneficiaries, include commitments and promises with respect to

maintaining and protecting the confidentiality of personal information set forth on Defendants' websites.

133. The OTP Data Breach revealed that Caresource and OTP breached their contractual promises to Plaintiffs and Class Members as set forth by the commitments and promises advertised on Defendants' websites.

134. Caresource and OTP breached their specific commitments to Plaintiffs and Class Members by failing to adhere to HIPAA and failing to ensure that vendors adhered to HIPAA.

135. Caresource and OTP breached their specific commitments to Plaintiffs and Class Members by failing to take reasonable safety measures to safeguard Plaintiffs' and Class Members' Private Information and ensuring vendors did same.

Plaintiffs' And Class Members' Damages

136. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

137. Plaintiffs' Private Information, including their sensitive PII and PHI, was compromised as a direct and proximate result of the Data Breach.

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

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

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

141. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

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

143. CareSource revealed that a subset of individuals affected by the Data Breach had additional Private Information that was compromised, including vital signs, medications, allergies, health screenings, and immunizations. When combined with publicly available information, this information would allow nefarious actors to paint a near complete health and personal history of Plaintiffs. Plaintiffs received identical letters from OTP and therefore cannot be assured that they are not among the subset of individuals with additional data that was compromised.

144. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid, or authorized their insurance companies to overpay, CareSource for a service that was intended to be accompanied by adequate data security, and, on information and belief, CareSource contracted with OTP to provide this service with Plaintiffs and Class Members as the intended third-party beneficiaries, but that information was not adequately protected by OTP. Part of the price Plaintiffs and Class Members paid to CareSource, and that it paid to OTP, was intended to be used by OTP to fund adequate security of OTP's computer property and protect Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for.

145. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

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

a. Finding fraudulent health care charges;

b. Purchasing credit monitoring and identity theft prevention;

c. Spending time on the phone with or at a healthcare organizations to dispute fraudulent charges;

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

e. Closely reviewing and monitoring health care accounts for unauthorized activity for years to come; and

f. Addressing personal medical information that could potentially become public.

147. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of OTP, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

148. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental— may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

149. Plaintiffs and Class Members face years of constant surveillance of their personal records, monitoring and loss of rights.

150. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and either have suffered harm or are at an imminent and increased risk of future harm.

CLASS ALLEGATIONS

151. Plaintiffs bring this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of themselves and on behalf of all other persons similarly situated (the "Class").

152. Plaintiffs propose the following Class definitions, subject to amendment as appropriate:

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

153. Excluded from each of the above Classes are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

154. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

155. Each of the proposed classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

156. Numerosity**.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of tens of thousands of individuals who have Caresource healthcare insurance and provided their Private Information to OTP, and whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Defendants' records, Class Members' records, publication notice, self-identification, and other means.

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

a. Whether Defendants engaged in the conduct alleged herein;
b. Whether Defendants' response was adequate;
c. Whether OTP unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;
d. Whether OTP failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
e. Whether OTP's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
f. Whether OTP's data security systems prior to and during the Data Breach were consistent with industry standards;
g. Whether Caresource had a duty to ensure OTP implemented adequate safeguards to protect the Private Information of Plaintiffs and Class Members;
h. Whether Caresource breached its duty by failing to ensure OTP implemented adequate safeguards to protect the Private Information of Plaintiffs and Class Members;

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

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

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

l. Whether Defendants had a legal duty to provide timely and accurate notice of the data breach to Plaintiffs and the Class Members;

m. Whether Defendants breached their duty to provide timely and accurate notice of the data breach to Plaintiffs and the Class Members;

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

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

p. Whether Defendants' conduct was negligent;

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

r. Whether Defendants were unjustly enriched;

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

t. Whether Defendants' conduct violated state laws;

u. Whether Plaintiffs and the other Class Members are entitled to additional credit or identity monitoring and are entitled to other monetary relief; and

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

158. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class member, was compromised in the Data Breach.

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

160. Predominance**.** OTP and Caresource have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was provided by Caresource to OTP, where OTP stored the data on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

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

162. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). OTP has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

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

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Nationwide Class or alternatively the Subclasses against Defendants Caresource and OTP)

164. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

165. Caresource knowingly collected and provided to OTP the Private Information of Plaintiffs and Class Members, and had a duty to ensure OTP exercised reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

166. OTP knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

167. Defendants knew, or should have known, of the risks inherent in collecting the Private Information of Plaintiffs and the Class Members and the importance of adequate security. Defendants knew or should have known that entities that maintain PHI are an attractive target for cyberattacks.

168. Defendants owed a duty of care to Plaintiffs and the Class Members whose Private Information was entrusted to it.

169. OTP's duties included, but were not limited to, the following:

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

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

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

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the Indiana Deceptive Consumer Sales Act and Ohio Consumer Sales Practices Act;

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

f. To promptly notify Plaintiff and the Class Members of the data breach, and to disclose precisely the type(s) of information compromise.

170. Caresource's duties included ensuring that its vendors, including OTP, carried out these duties by exercising reasonable diligence to safeguard Plaintiff's and Class Members' Private Information entrusted to Caresource and OTP.

171. Defendants knew that a breach of its systems, or the systems of its vendors, could damage hundreds of thousands of individuals, including Plaintiffs and the Class Members, and therefore had a duty to adequately protect their Private Information.

172. Plaintiffs and the Class Members were foreseeable and probable victims of any inadequate security practices, and Defendants owed them a duty of care not to subject them to an unreasonable risk of harm.

173. Defendants knew, or should have known, that the OTP computer systems did not adequately safeguard the Private Information of Plaintiff and the Class Members.

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

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

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

177. Defendants acted with reckless disregard for the rights of Plaintiffs and the Class Members by failing to provide prompt and adequate individual notice of the data breach so that they could take measures to protect themselves from damages caused by the fraudulent use the Private Information compromised in the data breach.

178. Defendants had a special relationship with Plaintiffs and the Class Members. Plaintiffs' and the Class Members' willingness to entrust Defendants with their Private Information was predicated on the understanding that Defendants would take adequate security precautions. Moreover, OTP had the ability to protect its systems (and the Private Information that it stored on them) from attack and Caresource had the obligation to ensure OTP implemented adequate protection of its systems from attack.

179. Defendants' breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised.

180. As a result of Defendants' ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members are unable to take all the necessary precautions to mitigate damages by preventing future fraud.

181. Defendants' breaches of duty caused a foreseeable risk of harm to Plaintiffs and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their Private Information.

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

183. Defendants also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and the Class Members' Private Information and promptly notify them about the data breach.

184. But for Defendants' wrongful and negligent breach of the duties it owed Plaintiffs and the Class Members, their Private Information either would not have been compromised or they would have been able to prevent some or all of their damages.

185. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and the Class Members have suffered damages and are at imminent risk of further harm.

186. The injury and harm that Plaintiffs and the Class Members suffered (as alleged above) was reasonably foreseeable.

187. The injury and harm that Plaintiffs and the Class Members suffered (as alleged above) was the direct and proximate result of Defendants' negligent conduct.

188. Plaintiffs and the Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

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

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Nationwide Class or alternatively the Subclasses against Defendants Caresource and OTP)

190. Plaintiffs restate and reallege the allegations in paragraphs 1-163 as if fully set forth herein.

191. Pursuant to Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

192. Pursuant to HIPAA, 42 U.S.C. § 1302d *et seq.*, Defendants had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information, and Caresource had a duty to ensure OTP did same.

193. Plaintiffs and the Class Members are within the class of persons that the FTCA and HIPAA were intended to protect.

194. Pursuant to the following state laws, Defendants operating in those states had a duty to those respective states' Plaintiffs and Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Private Information:

a. Indiana Deceptive Consumer Sales Act ("IDCSA"), Ind. Code § 24-5-0.5-3(a);

b. Ohio Insurance Transaction Information Standards Law, Ohio Rev. Code § 3904.13, § 3904.21(b);

c. Georgia Insurance Information and Privacy Protection Act, Ga. Code § 33-39-14, 21(b) *et seq.*, and

d. Georgia Data Breach Statute, Ga. Code Ann. § 10-1-912(a) *et seq.*

195. Plaintiffs and Class Members are within the class of persons these state laws were intended to protect.

196. Defendants breached their duties to Plaintiffs and Class Members under the FTCA, HIPAA, and state data security statutes by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information; and Caresource breached its duties to Plaintiffs and Class Members by failing to ensure OTP did same.

197. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se.*

198. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, they would not have been injured.

199. It was reasonably foreseeable, particularly given the growing number of data breaches of health information that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to OTP's email servers, networks, databases, and/or computers that stored or contained Plaintiffs' and Class Members' Private Information.

200. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered injury and are entitled to damages in the amount to be proven at trial.

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

COUNT III
BREACH OF CONTRACT
(On behalf of Plaintiffs and the Nationwide Class or alternatively the Subclasses against Defendants Caresource and OTP)

202. Plaintiffs restate and reallege the allegations in paragraphs 1-163 as if fully set forth herein.

203. Plaintiffs and Class Members purchased individual healthcare insurance policies from Caresource and entered into binding and enforceable contracts with Caresource.

204. All contracts between Caresource and Plaintiffs and Class Members were entered into prior to the OTP Data Breach.

205. The contracts between Plaintiffs and Class Members and Caresource were supported by consideration in many forms including the payment of premiums, contributions or fees by Plaintiffs and Class Members, and Plaintiffs and Class Members' performed under these contracts, including by providing their Private Information to Caresource as required.

206. Plaintiffs and Class Members fully performed their obligations under their contracts with Caresource and satisfied all conditions, covenants, obligations and promises of these agreements.

207. Caresource entered into binding and enforceable business associate agreements with OTP. Plaintiffs and Class Members were intended beneficiaries of these agreements that incorporated, either by express provision or by reference, the privacy and confidentiality policies pertaining to personal and health information provided by OTP to Caresource. Plaintiffs and Class Members sue in the alternative for breach of contract as third-party beneficiaries.

208. Caresource provided to OTP the Private Information of Plaintiffs and Class Members.

209. Caresource materially breached its contractual obligation to maintain and protect the confidentiality of Plaintiffs' and Class Members' Private Information from unauthorized disclosure by failing to ensure that OTP had adequate security to protect Plaintiffs' and Class Members' Private Information, and by failing to ensure that OTP's contractual obligations were met including protecting the confidentiality of Private Information.

210. OTP materially breached its contractual obligation to maintain and protect the confidentiality of Plaintiffs' and Class Members' Private Information from unauthorized disclosure by failing to implement and maintain adequate security to protect Plaintiffs' and Class Members' Private Information.

211. As a result of Defendants' breach of contract, Plaintiffs and Class Members did not receive the full benefit of the bargain, and instead received healthcare insurance and/or health care services that were less valuable than described in their contracts. Plaintiffs and Class Members were therefore damaged in an amount at least equal to the difference in value between that which was promised and the defective performance.

212. Also as a result of Defendants' breach of contract, Plaintiffs and Class Members have suffered actual damages resulting from the compromise and/or theft of their Private Information and remain at imminent risk of suffering additional damages in the future.

213. Also as a result of Defendants' breach of contract, Plaintiffs and Class Members have suffered actual damages resulting from their attempt to ameliorate the effect of the breach of contract and subsequent OTP Data Breach, including but not limited to have to purchase credit monitoring services or taking other steps to protect themselves from the loss of their Private Information.

214. Accordingly, Plaintiffs and Class Members have been injured as a result of Defendants' breach of contract and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV
BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On behalf of Plaintiffs and the Nationwide Class or alternatively the Subclasses against Defendants Caresource and OTP)

215. Plaintiffs restate and reallege the allegations in paragraphs 1-163 as if fully set forth herein.

216. Plaintiffs and Class Members entered into and were the beneficiaries of contracts with Caresource and its vendors.

217. These contracts were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and would not impair the rights of the other parties to receive their rights, benefits, and reasonable expectations under the contracts. These included the covenants that Caresource and OTP would act fairly, reasonably, and in good faith in carrying out their contractual obligations to protect the confidentiality of Plaintiffs' and Class Members' Private Information and to comply with industry standards and federal and state laws and regulations for the security of this information.

218. "Special relationships" exist between Caresource and OTP and the Plaintiffs and Class Members. Caresource entered into a "special relationship" with those Plaintiffs and Class

Members who purchased insurance plans from them and/or enrolled in health services plans with them and who entrusted their confidential Private Information to Caresource and its vendors.

219. As set forth above in the breach of contract claim, Caresource and OTP promised to take specific measures to protect Plaintiffs' and Class Members' Private Information. Even if Caresource is held not to have breached any express promise in these contracts, Caresource and OTP breached the covenant of good faith and fair dealing by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class Members' Private Information, resulting in the OTP Data Breach. Caresource and OTP unreasonably interfered with the contract benefits owed to Plaintiff and Class Members by: compiling and storing Plaintiff and Class Members' data in a Database that was not adequately protected; by failing to implement reasonable and adequate security measures consistent with industry standards to protect and limit access to the Private Information in the OTP Database; by permitting unauthorized access to all the Private information in this Database; and by failing to implement reasonable auditing procedures to detect and halt the unauthorized encryption and extraction of data.

220. Plaintiffs and Class Members performed all conditions, covenants, obligations, and promises owed to Caresource and OTP, including paying Caresource premiums for their insurance and health benefits contracts and providing Caresource and its vendors the confidential information required by the contracts.

221. As a result of Caresource and OTP's breach of the implied covenant, Plaintiffs and Class Members did not receive the full benefit of their bargain, and instead received health insurance and/or health care services and related services that were less valuable than what they paid for and less valuable than their reasonable expectations under the contracts. Plaintiffs and Class Members were damaged in an amount at least equal to the difference in value between that which they reasonably expected under the contracts and Caresource and OTP's partial, deficient and/or defective performance.

222. Also as a result of Caresource and OTP's breach of the covenant of good faith and fair dealing, Plaintiffs and Class Members have suffered actual damages resulting from the

compromise and/or theft of their Private Information and remain at imminent risk of suffering additional damages in the future.

223. Also as a result of Caresource and OTP's breach of the covenant of good faith and fair dealing, Plaintiffs and Class Members have suffered actual damages resulting from their attempt to ameliorate the effect of the breach and the subsequent OTP Data Breach, including but not limited to purchasing credit monitoring services or taking other steps to protect themselves from the loss of their Private Information.

224. Accordingly, Plaintiffs and Class Members have been injured as a result of Caresource and OTP's breaches of the covenant of good faith and fair dealing and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT V
VIOLATION OF INDIANA DECEPTIVE CONSUMER SALES ACT
IND. CODE §§ 24-5-0.5-0.1 *et seq.*
(On behalf of Plaintiff Gibson and the Indiana Class against Defendants Caresource and OTP)

225. Plaintiff Gibson restates and realleges the allegations in paragraphs 1-163 as if fully set forth herein.

226. Indiana's Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5-3(a) ("IDCSA") prohibits suppliers from engaging in deceptive, unfair, and abusive acts or omissions in consumer transactions.

227. A "Health maintenance organization" for purposes of Indiana law means "a person that undertakes to provide or arrange for the delivery of health care services to enrollees on a prepaid basis, except for enrollee responsibility for copayments or deductibles." Ind. Code §27-13-1-19. The purchase of health care services from an HMO is not "insurance" under Indiana law, and a contract for payment for health services from an HMO, as defined in Ind. Code §27-13-1-10, is not a "contract of insurance."

228. "Contracts of insurance" are exempt from the Indiana Deceptive Consumer Sales Act, but the pre-paid health benefits sold by HMOs and the administrative services provided by

Defendants to Plaintiff Gibson and the Indiana Class are "consumer transactions" within the coverage of that Act, and Defendants selling HMO and administrative services are "suppliers." Ind. Code § 24-5-0.5-2(a)(1), (3), (4).

229. Defendants are "suppliers" who engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of "consumer transactions" pertaining to the purchase and sale of administrative services to Plaintiff Gibson and the Indiana Class, in violation of Ind. Code § 24-5-0.5-3, including but not limited to the following:

a. Defendants misrepresented and fraudulently advertised material facts pertaining to the HMO and administrative services to Plaintiff Gibson and the Indiana Class by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff Gibson's and the Indiana Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft;

b. Defendants misrepresented material facts pertaining to HMO and administrative services to Plaintiff Gibson and the Indiana Class by representing and advertising that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff Gibson and the Indiana Class Members' Private Information;

c. Defendants omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for Plaintiff Gibson and the Indiana Class Members' Private Information;

d. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff Gibson and the Indiana Class Members' Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the OTP Data Breach. These unfair acts and practices

violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45), HIPAA (42 U.S.C. § 1302d et. seq.), Indiana's HMO Confidentiality law (Ind. Code §27-13-31-1), and Indiana's data breach statute (§ 24-4.9-3.5);

e. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the OTP Data Breach to Plaintiff Gibson and the Indiana Class Members in a timely and accurate manner, contrary to the duties imposed by Ind. Code § 24-4.9-3.3;

f. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the OTP Data Breach to enact adequate privacy and security measures and protect Plaintiff Gibson and the Indiana Class Members' Personal Information from further unauthorized disclosure, release, data breaches, and theft.

230. As a direct and proximate result of Defendants' deceptive trade practices, Plaintiff Gibson and the Indiana Class Members suffered injuries, including the loss of their legally protected interest in the confidentiality and privacy of their Private Information, and damages.

231. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

232. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiff Gibson and the Indiana Class Members' Private Information and that risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff Gibson and members of the Indiana Class.

233. Plaintiff Gibson and the Indiana Class Members seek relief under Ind. Code §24-5-0.5-4, including, not limited to damages, restitution, penalties, injunctive relief, and/or attorneys' fees and costs. Senior Members of the Indiana Class injured by Defendants' unfair and deceptive trade practices also seek treble damages, pursuant to § Ind. Code §24-5-0.5-4(i).

COUNT VI
OHIO INSURANCE TRANSACTION INFORMATION STANDARDS LAW
OHIO REV. CODE § 3904.13, § 3904.21(b)
(On behalf of Plaintiff King and the Ohio Subclass against Defendants Caresource and OTP)

234. Plaintiff King restates and realleges the allegations in paragraphs 1-163 as if fully set forth herein.

235. Plaintiff King brings this claim against Defendants Caresource and OTP operating in Ohio on behalf of the Ohio Class whose personal information was compromised as a result of the OTP Data Breach.

236. Defendants are "insurance institution[s]" for purposes of the Insurance Transaction Information Standards Law, Ohio Rev. Code § 3904.13.

237. Defendants collected and received individually identifiable Private Information regarding Plaintiff King and members of the Ohio Class during insurance transactions.

238. Defendant OTP disclosed individually-identifiable Private Information regarding Plaintiff King and members of the Ohio Class that was collected or received in connection with an insurance transaction without their authorization, in violation of Ohio Rev. Code § 3904.13. The disclosure of Private Information to unauthorized individuals in the OTP Data Breach resulted from the actions or omissions of Caresource and OTP employees. Thus, Defendants actively and affirmatively allowed the cyberattackers to see and obtain individually-identifiable Private Information regarding Plaintiff King and members of the Ohio Class.

239. The OTP Data Breach compromised Private Information, including PHI, and violated the rights of Plaintiff King and members of the Ohio Class. Defendants' illegal disclosure

and failure to maintain the confidentiality of their Private Information in violation of Ohio Rev. Code § 3904.13.

240. Plaintiff King and the Ohio Class seek relief under Ohio Rev. Code §3904.21, including but not limited to actual damages, nominal damages, injunctive relief, and/or attorneys' fees and costs.

COUNT VII
GEORGIA INSURANCE INFORMATION AND PRIVACY PROTECTION ACT
GA. CODE § 33-39-14, 21(b) *et seq.*
(On behalf of Plaintiff Strickland and the Georgia Subclass against Defendants Caresource and OTP)

241. Plaintiff Strickland restates and realleges the allegations in paragraphs 1-163 as if fully set forth herein.

242. Plaintiff Strickland brings this claim against Defendants operating in Georgia on behalf of the Georgia Class whose personal information was compromised as a result of the OTP Data Breach.

243. Defendants are "insurance institution[s]" for purposes of the Georgia Insurance Information and Privacy Protection Act, Ga. Code §33-39-14.

244. Defendants collected and received individually-identifiable Private Information regarding Plaintiff Strickland and members of the Georgia Class during insurance transactions.

245. Defendant OTP disclosed individually-identifiable Private Information regarding Plaintiff Strickland and members of the Georgia Class that was collected or received in connection with an insurance transaction without their authorization, in violation of Ga. Code §33-39-14. The disclosure of Private Information to unauthorized individuals in the OTP Data Breach resulted from the actions or omissions of Caresource and OTP employees. Thus, Defendants actively and affirmatively allowed the cyberattackers to see and obtain individually-identifiable Private Information regarding Plaintiff Strickland and members of the Georgia Class. The OTP Data Breach compromised Private Information, including PHI, and violated the rights of Plaintiff Strickland and members of the Georgia Class.

246. Plaintiff Strickland and the Georgia Class have suffered damages from Defendants' illegal disclosure and failure to maintain the confidentiality of their personal information.

247. Plaintiff Strickland and the Georgia Class seeks relief under Ga. Code §33-39-21(b), including but not limited to actual damages, nominal damages, injunctive relief, and/or attorneys' fees and costs.

COUNT VIII
GEORGIA DATA BREACH STATUTE
GA. CODE ANN. § 10-1-912(a) *et seq.*
(On behalf of Plaintiffs and the Georgia Subclass against Defendants Caresource and OTP)

248. Plaintiff Strickland restates and realleges the allegations in paragraphs 1-163 as if fully set forth herein.

249. Defendants Caresource and OTP are required to accurately notify Plaintiff Strickland and Georgia Class Members if Defendants become aware of a breach of their data security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff Strickland's and Georgia Class Members' Personal Information) in the most expedient time possible and without unreasonable delay under Ga. Code Ann. § 10-1-912(a).

250. Defendants are businesses that own or license computerized data that includes personal information as defined by Ga. Code Ann. § 10-1-912(a).

251. Plaintiff Strickland and Georgia Class Members' Personal Information (e.g., Member ID number) includes personal information as covered under Ga. Code Ann. § 10-1-912(a)

252. Because Defendants were aware of a breach of the OTP security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiff Strickland's and Georgia Class Members' Personal Information), Defendants had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Ga. Code Ann. § 10-1-912(a).

253. Thus, by failing to disclose the OTP Data Breach in a timely and accurate manner, Defendants violated Ga. Code Ann. § 10-1-912(a).

254. As a direct and proximate result of Defendants' violations of Ga. Code Ann. § 10-1-912(a), Plaintiff Strickland and Georgia Class Members suffered damages, as described above.

255. Plaintiff Strickland and Georgia Class Members seek relief under Ga. Code Ann. § 10-1-912 including, but not limited to, actual damages and injunctive relief.

COUNT IX
NEGLIGENT MISREPRESENTATION
(On behalf of Plaintiffs and the Nationwide Class or alternatively the Subclasses against Defendant Caresource)

256. Plaintiffs restate and reallege the allegations in paragraphs 1-163 as if fully set forth herein.

257. Defendant Caresource negligently and recklessly misrepresented material facts, pertaining to the sale of insurance and health benefits services, to Plaintiffs and Class Members by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs and Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft.

258. Defendant Caresource negligently and recklessly misrepresented material facts, pertaining to the sale of insurance and health benefits services, to Plaintiffs and Class Members by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiffs' and Class Members' Private Information.

259. Defendant Caresource either knew or should have known that their representations were not true.

260. In reliance upon these misrepresentations, Plaintiffs and Class Members purchased insurance or health benefits services from Defendant Caresource.

261. Had Plaintiffs and Class Members, as reasonable persons, known of Defendant Caresource's inadequate data privacy and security practices, or that Defendant was failing to ensure OTP was in compliance with the requirements of federal and state laws pertaining to the privacy and security of Class Members' Private Information, they would not have purchased

insurance or health benefits services from Defendant Caresource, and would not have entrusted their Private Information to Caresource.

262. As direct and proximate consequence of Defendant Caresource's negligent misrepresentations, Plaintiffs and Class Members have suffered the injuries alleged above.

COUNT X
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class or alternatively the Subclasses against Defendants Caresource and OTP)

263. Plaintiffs restate and reallege the allegations in paragraphs 1-163 as if fully set forth herein.

264. This count is plead in the alternative to Count III above.

265. Defendants have retained the benefits of their unlawful conduct including the amounts received for data and cybersecurity practices that they did not provide. Due to Defendants' conduct alleged herein, it would be unjust and inequitable under the circumstances for Defendants to be permitted to retain the benefit of their wrongful conduct.

266. The premiums for health insurance and health benefits services that Plaintiffs and Class Members paid (directly or indirectly) to Defendants should have been used by Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

267. Plaintiffs and Class Members are entitled to full refunds, restitution and/or damages from Defendants and/or an order of this Court proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. If necessary, the establishment of a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation may be created.

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

269. Plaintiffs and the Class Members conferred a benefit on Defendants by paying for data and cybersecurity procedures to protect their Private Information that they did not receive.

COUNT XI
DECLARATORY JUDGMENT
(On behalf of Plaintiffs and the Nationwide Class or alternatively the Subclasses)

270. Plaintiffs restate and reallege the allegations in paragraphs 1-163 as if fully set forth herein.

271. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statute described in this Complaint.

272. Defendants owe a duty of care to Plaintiffs and the Class Members which required it to adequately secure Private Information and ensure its vendors did same.

273. OTP still possesses Private Information regarding Plaintiffs and the Class Members.

274. Plaintiffs allege that OTP's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

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

a. Defendants owe a legal duty to secure Plaintiffs' and Class Members' Private Information and to timely disseminate notice of a data breach under the common law and Section 5 of the FTCA;

b. Defendants are in breach of their duties of care to provide reasonable security procedures and practices appropriate to the nature of the

information to protect Plaintiffs' and Class Members' Private Information; and

c. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure Plaintiffs' and Class Members' Private Information.

276. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect Plaintiffs' and Class Members' Private Information, including the following:

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

b. Order OTP to comply with its obligations and duties of care, including, but not limited to:

i. Not to use or further disclose the information other than as permitted by the contract or as required by law;

ii. Implement appropriate safeguards to prevent unauthorized uses or disclosures of the PHI;

iii. Report any use or disclosure not provided for by the agreement, including breaches of unsecured PHI;

iv. Satisfy individuals' requests for copies of PHI, incorporate any amendments, and account for the disclosure;

v. Return or destroy PHI received from, created for, or received on behalf of, Caresource at the termination of the agreement; and

vi. Ensure that any with access to PHI agree to the same restrictions and conditions that apply to Caresource.

c. Order Caresource to comply with its obligations and duties of care, including, but not limited to:

i. Conduct an accurate and thorough risk and vulnerability assessment of Caresource and OTP procedures to safeguard PHI;

ii. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level;

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

iv. Obtain satisfactory assurances that OTP would properly safeguard PHI provided by Caresource;

v. Perform a periodic evaluation of OTP security policies and procedures; and

vi. Maintain records of periodic assessments of OTP policies and procedures.

277. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at OTP. The risk of another such breach is real, immediate, and substantial. If another breach at OTP occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

278. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

279. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at OTP, thus eliminating the additional injuries that would result to Plaintiffs and Class Members whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes described above, seek the following relief:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Classes requested herein;

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

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

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

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

f. A judgment in favor of Plaintiffs and the Classes awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law, and

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

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: September 26, 2022

Respectfully submitted,

/s/ Christopher Wiest
Christopher Wiest (OH 0077931)
Chris Wiest, Atty at Law, PLLC
25 Town Center Blvd, Suite 104
Crestview Hills, KY 41017
Tel: (513) 257-1895
Fax: (859) 495-0803
E: chris@cwiestlaw.com

Mason A. Barney (*pro hac vice* to be filed)
Sean Nation (*pro hac vice* to be filed)
Ursula Smith (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: snation@sirillp.com
E: usmith@sirillp.com